Kosten- und Nutzenbetrachtungen im IT-Sicherheitsmanagement

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg

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

Zu hohe oder zu niedrige Ausgaben?

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

vs.

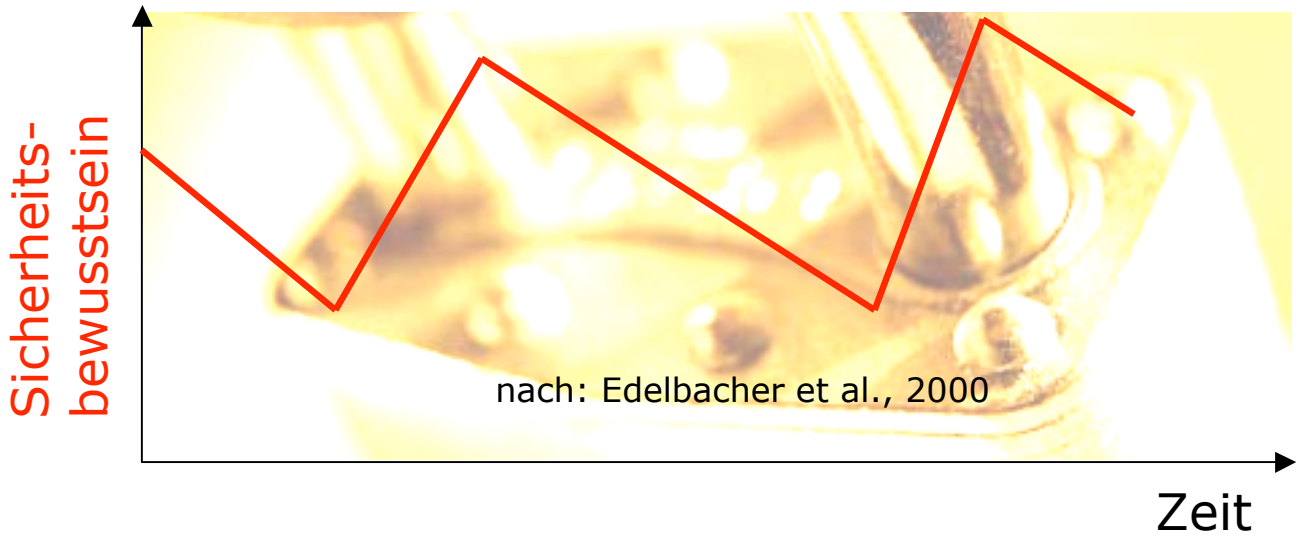
»The greatest IT risk facing most companies is more prosaic than a catastrophe. It is, simply, overspending.«
Nicolas G. Carr

- 2 Perspektiven
  - Sicherheit eines Produktes
  - Sicherheit eines Unternehmens → Fokus des Vortrags

Erste mögliche 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

Sicherheit: Abgrenzung von Security & Safety

SECURITY
Schutz gegen beabsichtigte Angriffe

Vertraulichkeit
- Abhörsicherheit
- Sicherheit gegen unbefugten Gerätezugriff
- Anonymität
- Unbeobachtbarkeit

Integrität
- Übertragungsintegrität
- Zurechenbarkeit
- Abrechnungsintegrität

Verfügbarkeit
- Ermöglichen von Kommunikation

SAFETY
Schutz vor unbeabsichtigten Ereignissen

Fehlertoleranz

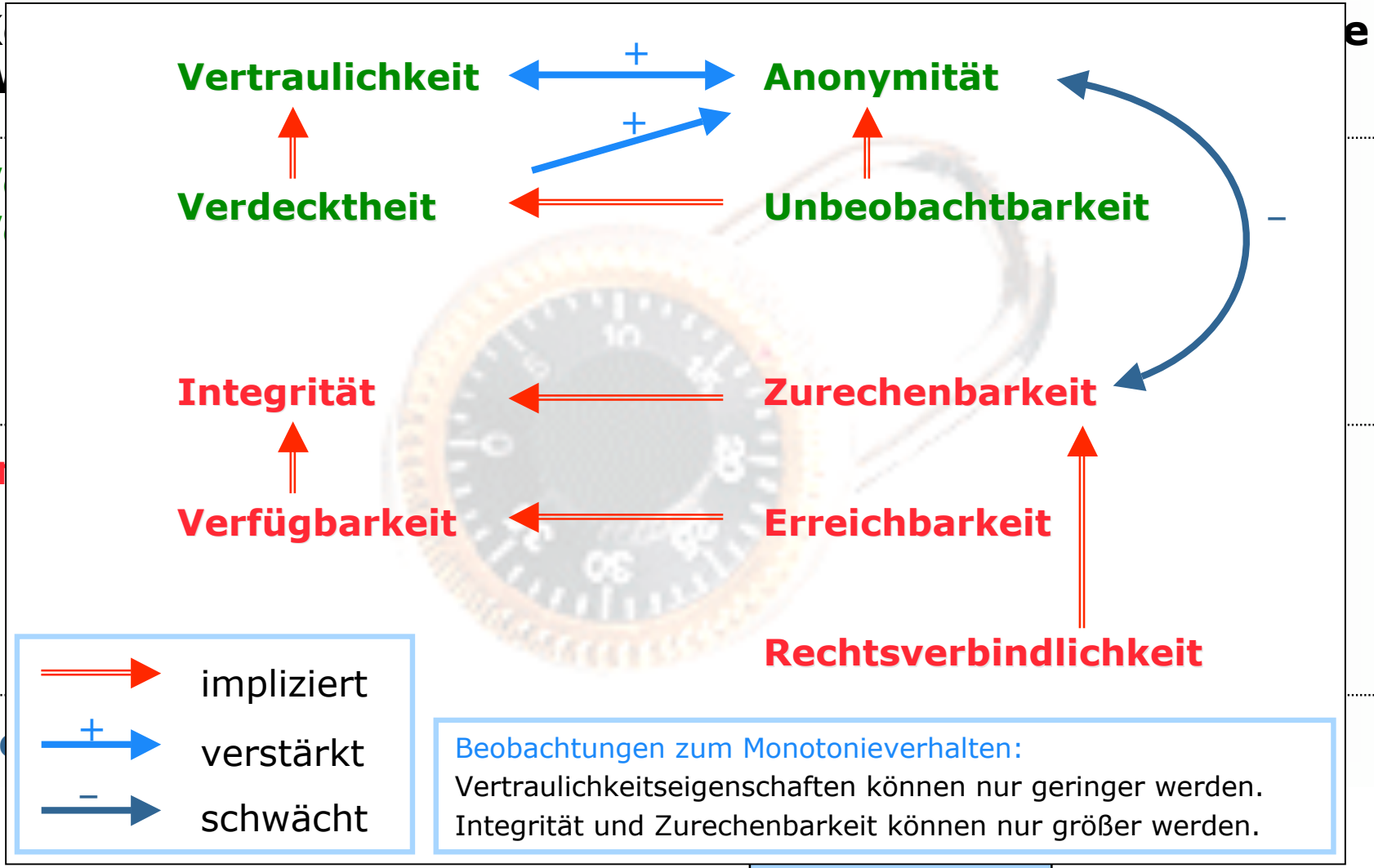
Verfügbarkeit
- Funktionssicherheit
- Technische Sicherheit
- Schutz vor Überspannung, Überschwemmung, Temperaturschwankungen
- Schutz vor Spannungsausfall

Sonstige Schutzziele
- Maßnahmen gegen hohe Gesundheitsbelastung
- …

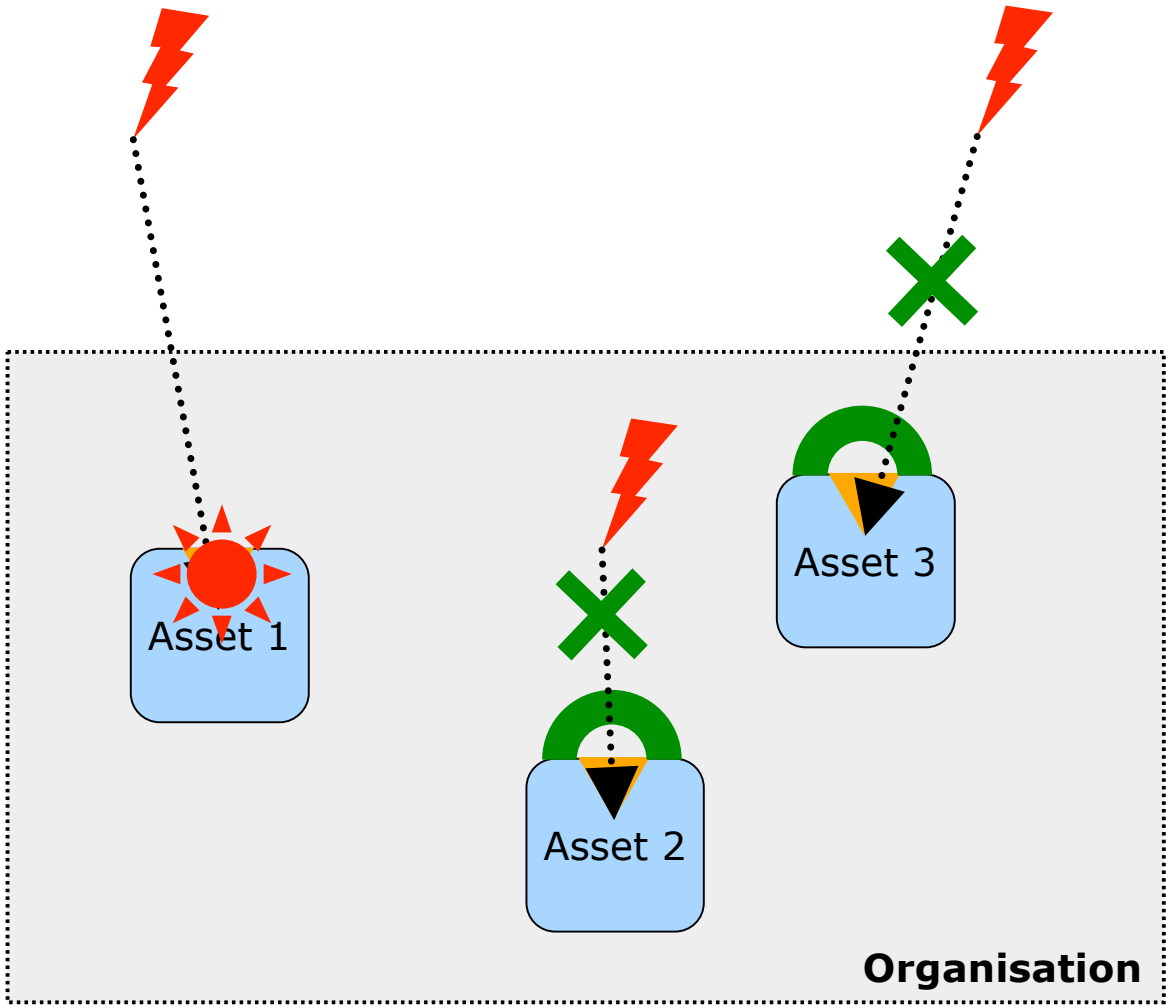
Was ist zu schützen?

Kommunikationsgegenstand WAS?		**Kommunikationsumstände WANN?, WO?, WER?**
Vertraulichkeit **Verdecktheit**	**Inhalte**	**Anonymität** **Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**
Integrität	**Inhalte**	**Zurechenbarkeit** **Rechtsverbindlichkeit** **Absender** **Bezahlung** **Empfänger**
Verfügbarkeit	**Inhalte**	**Erreichbarkeit** **Nutzer** **Rechner**

Was ist zu schützen?



Von der Bedrohung zum Sicherheitsvorfall



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

Verwundbarkeiten, z.B.
- Konfigurationsfehler
- Buffer Overflows

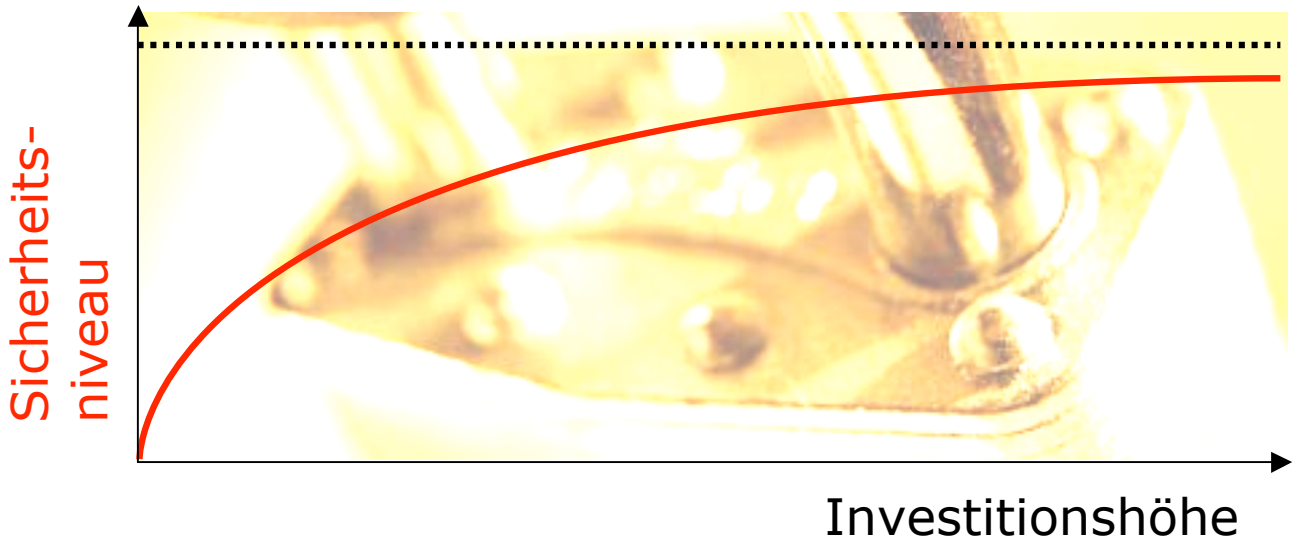
Schutzziele
- Vertraulichkeit
- Verfügbarkeit
- Integrität

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

Zweite mögliche Antwort

So viel wie man braucht, um total sicher zu sein

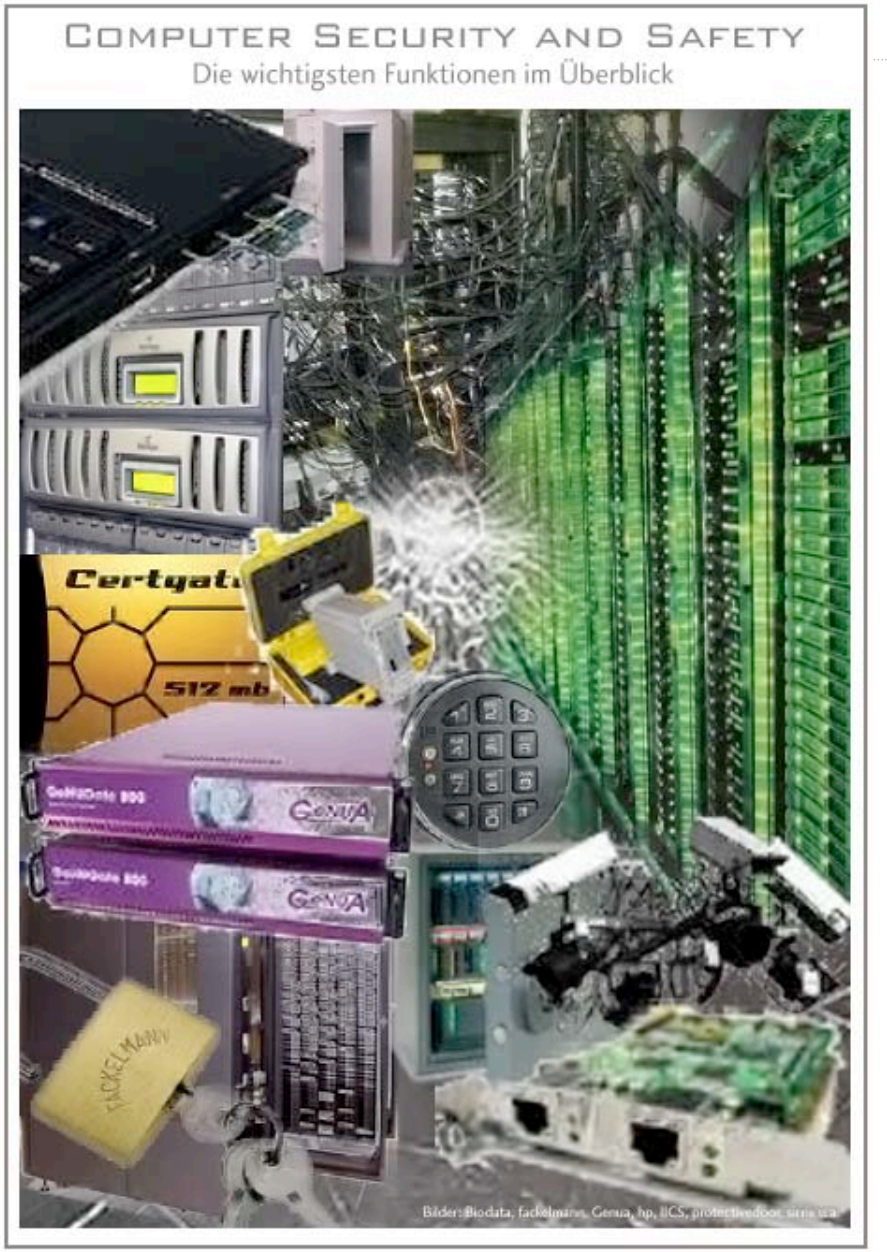
- Kritik:
  - 100 %-ige Sicherheit ist nicht erreichbar



Dritte mögliche Antwort

So viel wie das Budget hergibt

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



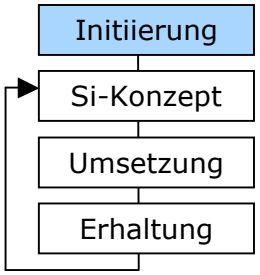
Unterschiedliche Zielsetzungen

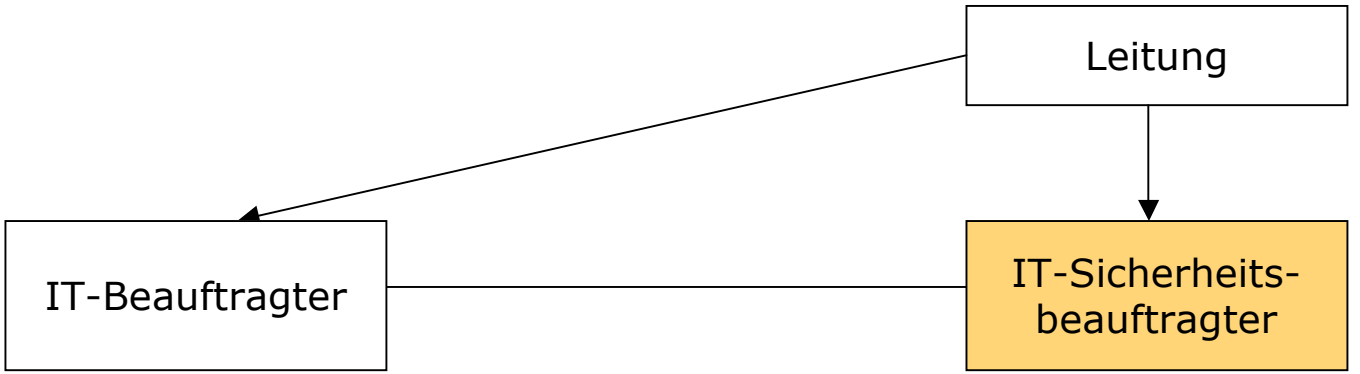
- Ziel Unternehmensleitung
  - Ausgaben gering halten
  - Kosten einsparen
  - Nur Projekte mit sichtbarem Nutzen realisieren

- 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.

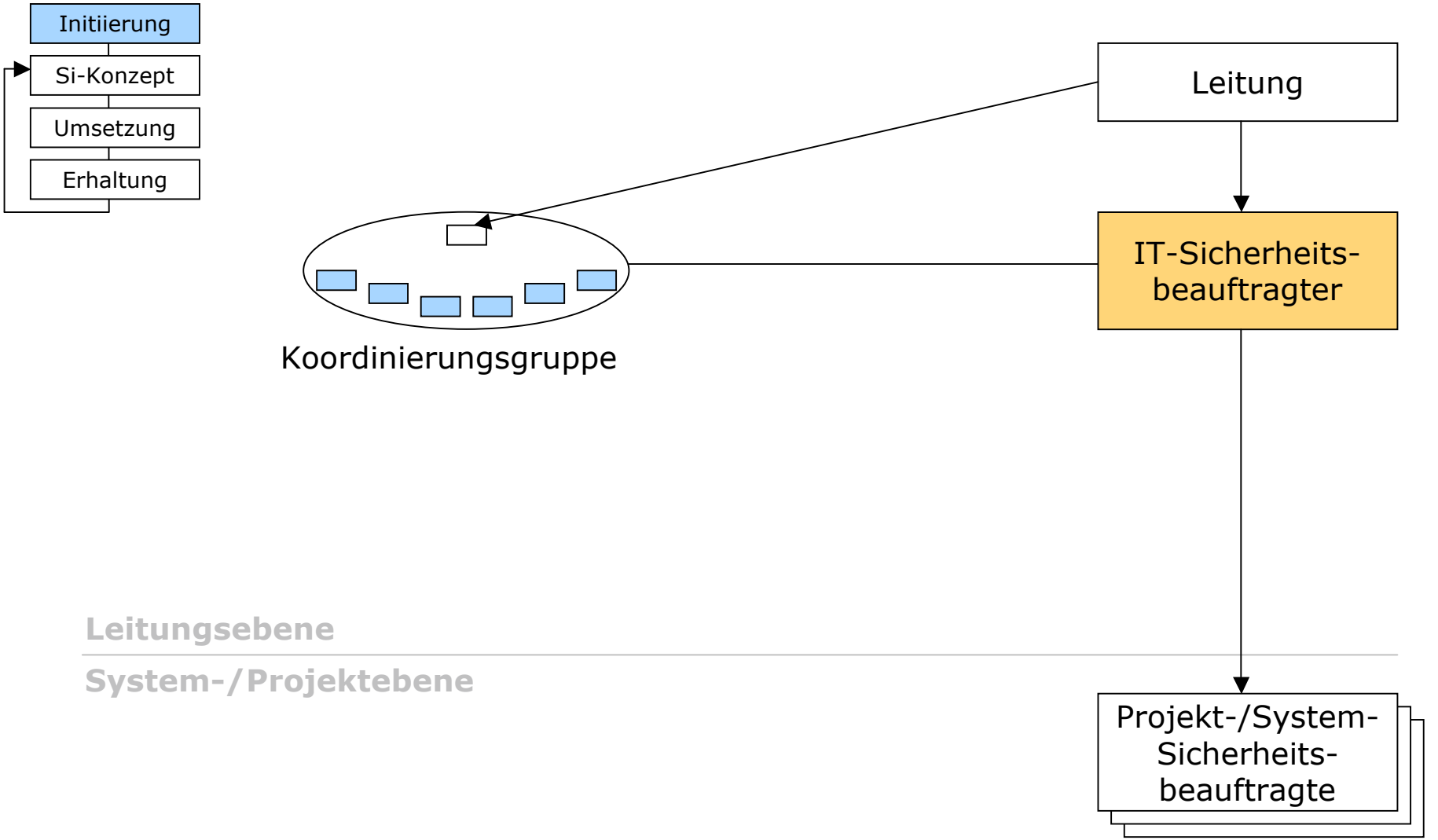
Organisationsstruktur für IT-Sicherheit: *Kleine Organisationen*





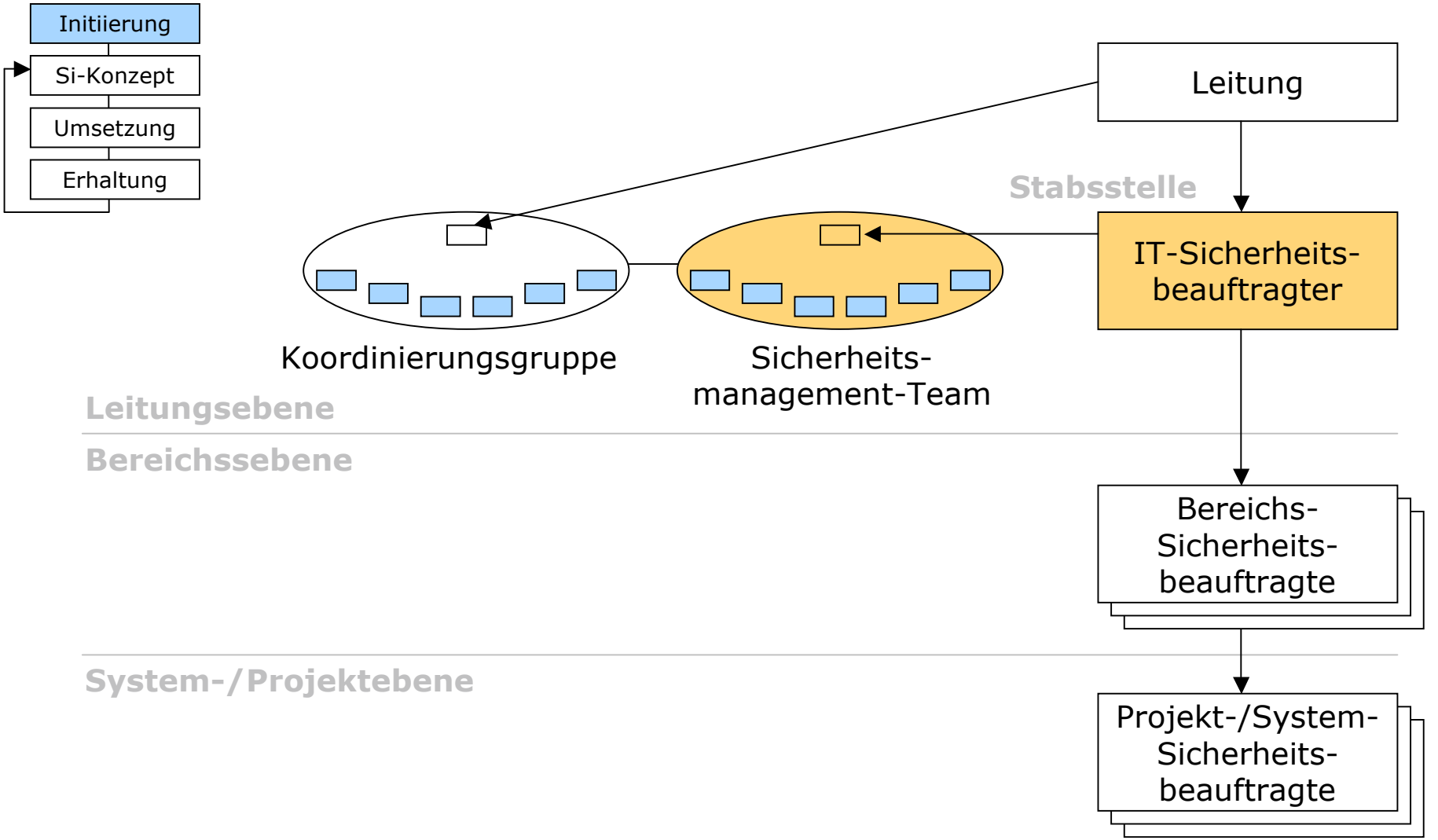
nach: GSHB, M2.193

Organisationsstruktur für IT-Sicherheit: *Mittlere Organisationen*



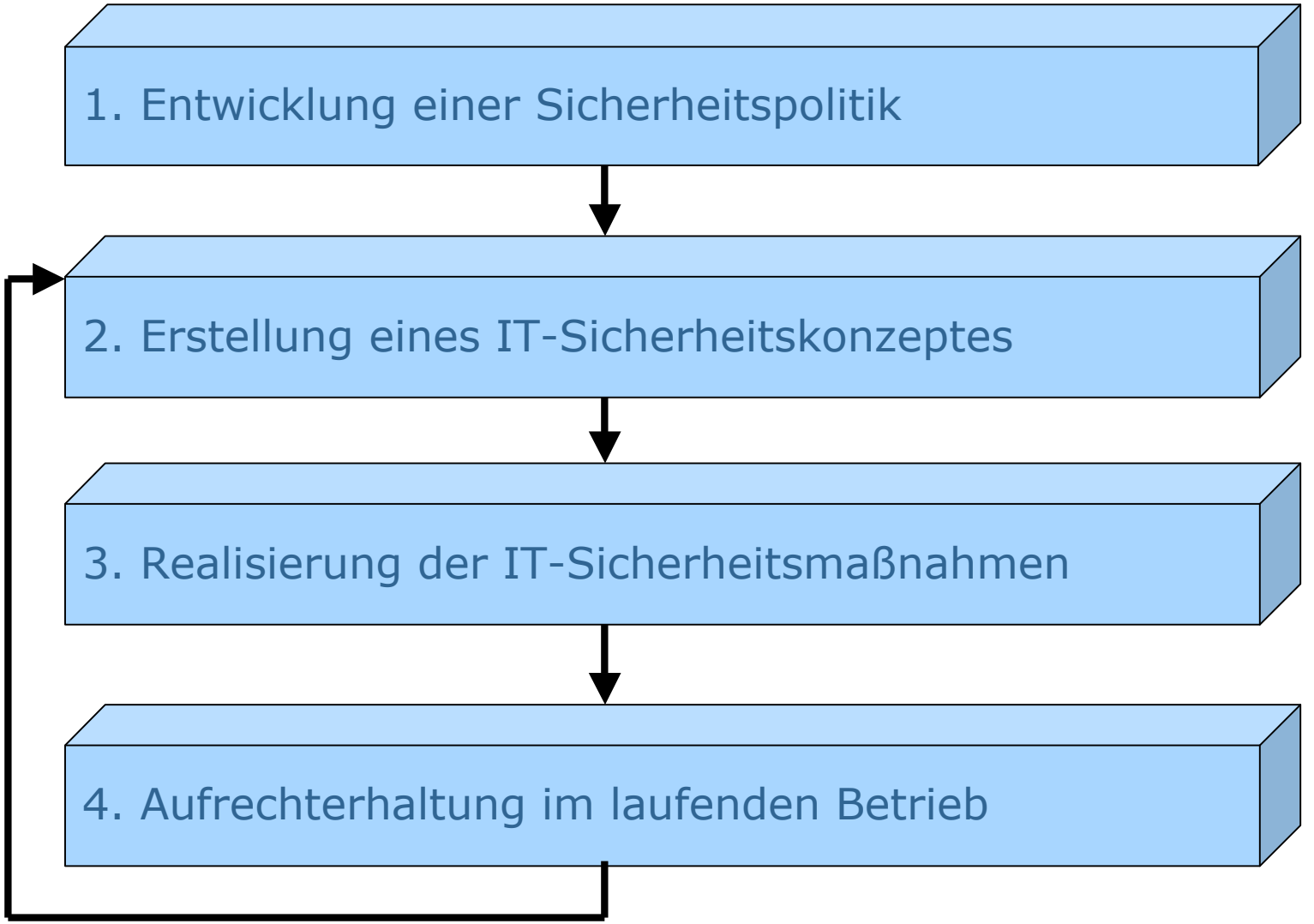
nach: GSHB, M2.193

Organisationsstruktur für IT-Sicherheit: *Große Organisationen*



nach: GSHB, M2.193

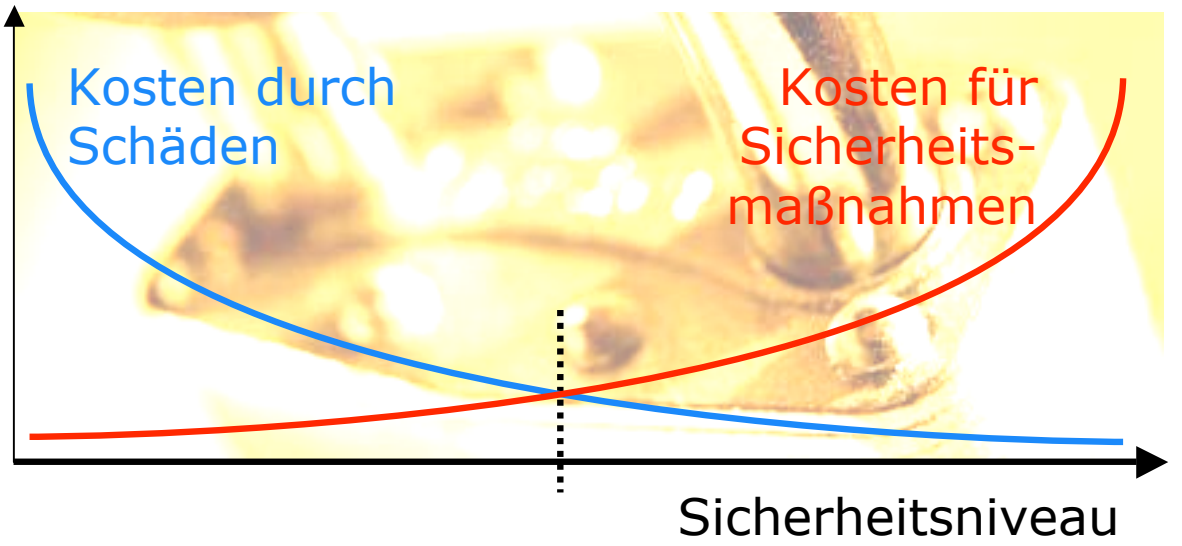
Sicherheitsmanagement-Vorgehensmodell



Vierte mögliche 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 mögliche 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 mögliche Antwort (1)

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

- ROSI
  - Return on Security Investment
  - basiert auf dem Konzept der Berechnung einer jährlichen Verlusterwartung aus den 70er Jahren
  - soll Analogie zum klassischen Return on Investment herstellen
  - verschiedene Darstellungsformen und Weiterentwicklungen

„Nobody tries to quantify the ROI of air conditioning. So why try it with security?“ Jay G. Heiser: Security Through ROSI-colored Glasses, in: Information Security, Juli 2002

Return on Security Investment (ROSI)

- Basiert auf der Berechnung einer jährlichen Verlusterwartung (einzelnes Ereignis): (FIBS 1979)

$$ALE = SLE \cdot ARO$$

ALE: annual loss expectancy

SLE: single loss expectancy

ARO: annual rate of occurrence

- Aggregation von ALEs mehrerer Ereignisse: (Soo Hoo 2000)

$$ALE = \sum_{i=1}^{n} S(O_i)F_i$$

O_i: harmful outcome i

$S(O_i)$: Severity of O_i (in monetary units)

- Return on security investment: (Wei et. al 2001)

$$ROSI = ALE_0 - ALE_1 - \text{cost}$$

ALE_0-ALE_1: change of the ALE from year 0 to year 1

Cost: cost of the security measure

- Wenn ROSI >0, dann war die Investition nützlich.

Return on Security Investment (ROSI)

- ROSI
  - Alternative Berechnung als Verhältnisgleichung: (Sonnenreich et. al. 2006)

$$ROSI = \frac{(\text{risk exposure} \cdot \%\ \text{risk mitigated}) - \text{cost}}{\text{cost}}$$

  - Weitere Variante: (Pfleeger and Pfleeger 2003)

$$\text{risk leverage} = \frac{(\text{risk exp. before red.}) - (\text{risk exp. after red.})}{\text{cost of risk reduction}}$$

difference of risk exposure before and after reduction in relation to the costs of the measure

- Vorteile
  - Vergleichbarkeit verschiedener Sicherheitsmaßnahmen
  - Vergleichbarkeit der Investitionen in Sicherheitsmaßnahmen mit anderen Investitionen (außerhalb der IT-Sicherheit)

Fünfte mögliche 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

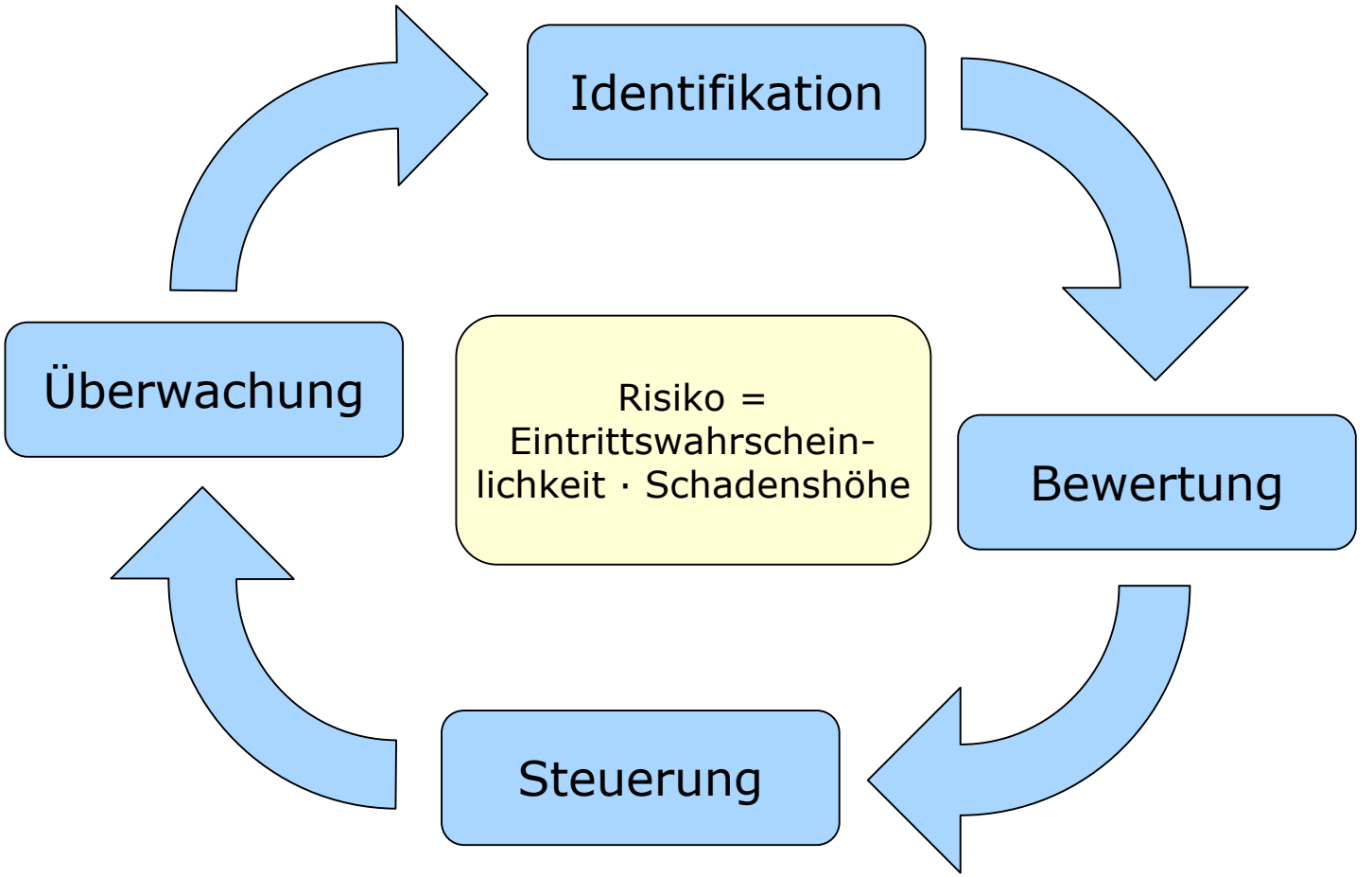
Sicherheitsmanagement beginnt auf der Strategieebene

	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

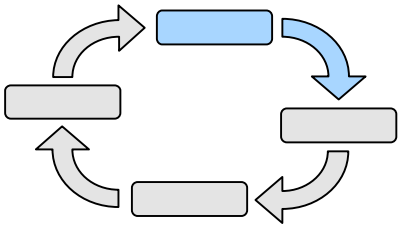
- Aussagen für die strategische Ebene
  - Wer nur auf vorgefertigte Lösungen setzt, verliert auf lange Sicht wertvolles Know How.
  - Heterogene IT-Landschaften schützen vor Kumulrisiken.
  - IT-Sicherheit ist mehr als nur Technik.
  - Sicherheit sollte von Beginn an integraler Bestandteil der Prozesse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

Risikomanagement Kreislauf

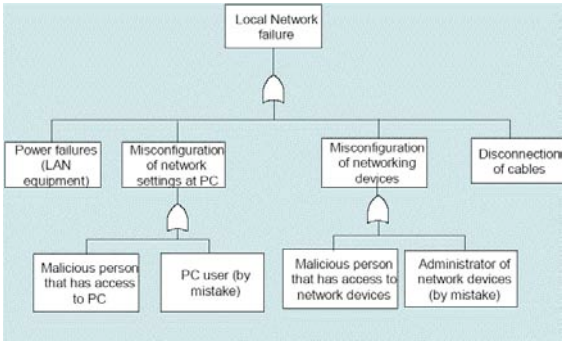


Identifikation von Bedrohungen

- Frage
  - »Welche Bedrohungen sind für das jeweilige Schutzobjekt relevant? «



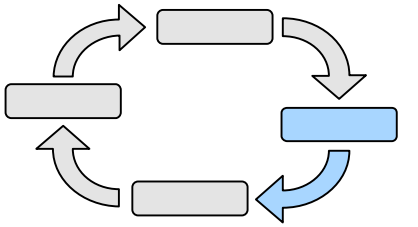
- Methoden & Werkzeuge
  - OCTAVE-Methodik, CORAS-Framework
  - Checklisten
  - Workshops
  - Fehlerbäume, Attack-Trees
  - Szenarioanalysen



- Herausforderungen
  - Vollständige Erfassung aller Bedrohungen

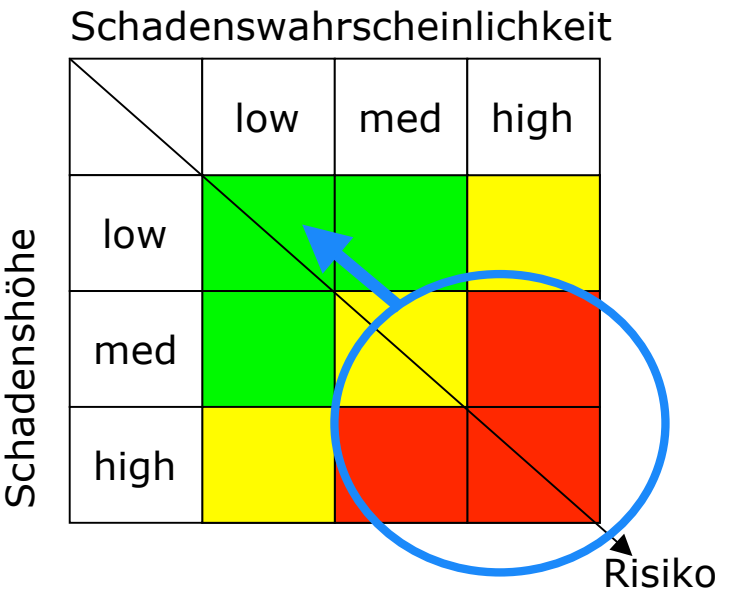
Bewertung von Risiken

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



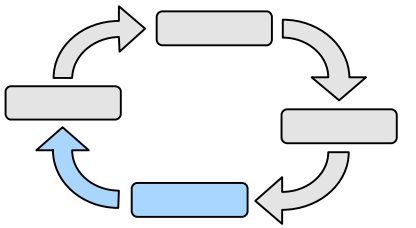
- Methoden & Werkzeuge
  - Qualitative Bewertung
  - Quantitative Bewertung
  - Spieltheorie
  - Maximalwirkungsanalyse

- Herausforderungen
  - Abhängigkeit von den Assets
  - Strategische Angreifer
  - Korrelationen
  - Quantifizierbarkeit



Steuerung der Risiken

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



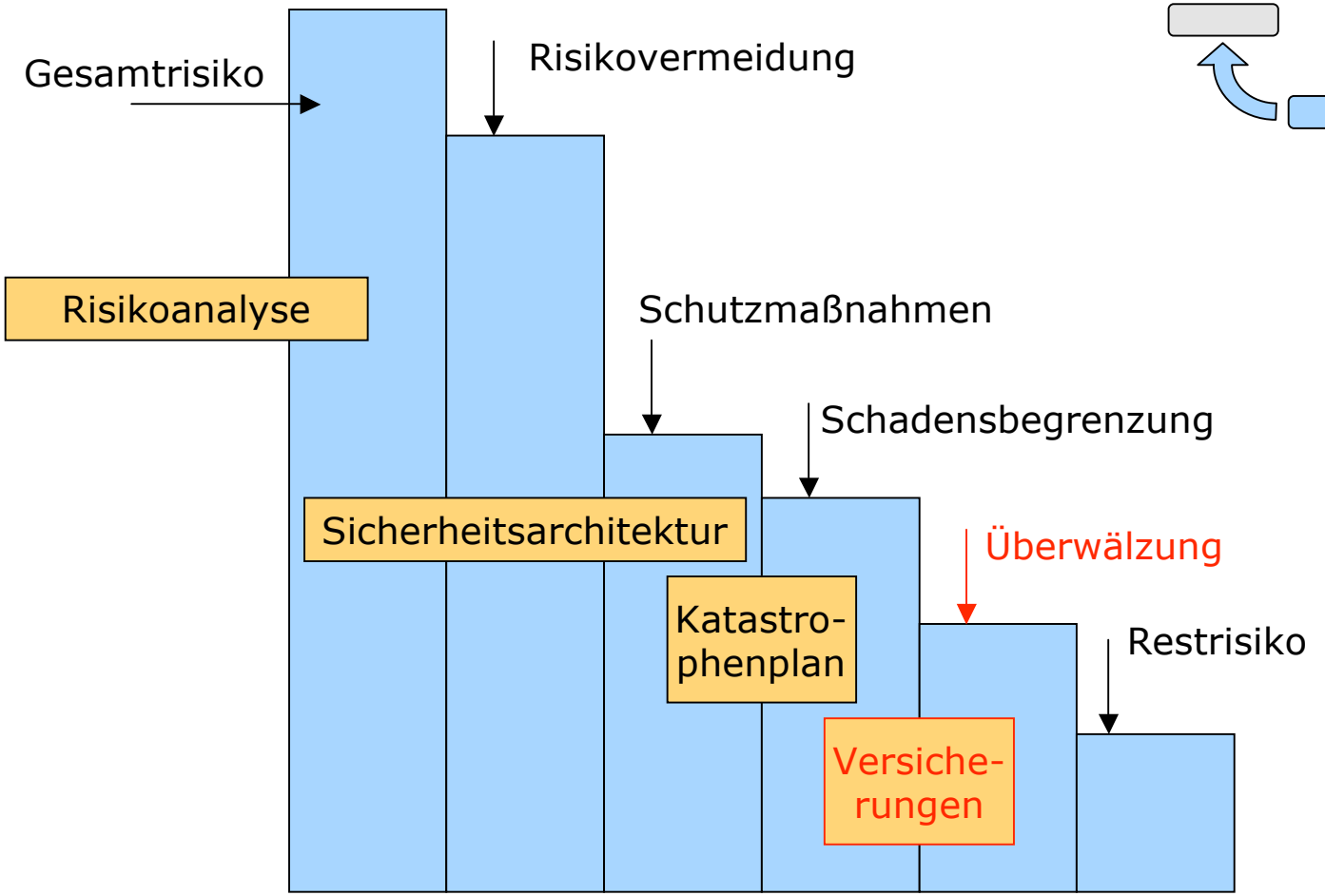
- Methoden
  - Best Practice Ansätze / Grundschutz
  - Hilfsmittel aus der Investitionsrechnung und Entscheidungstheorie, z.B. NPV, IRR, AHP

- 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

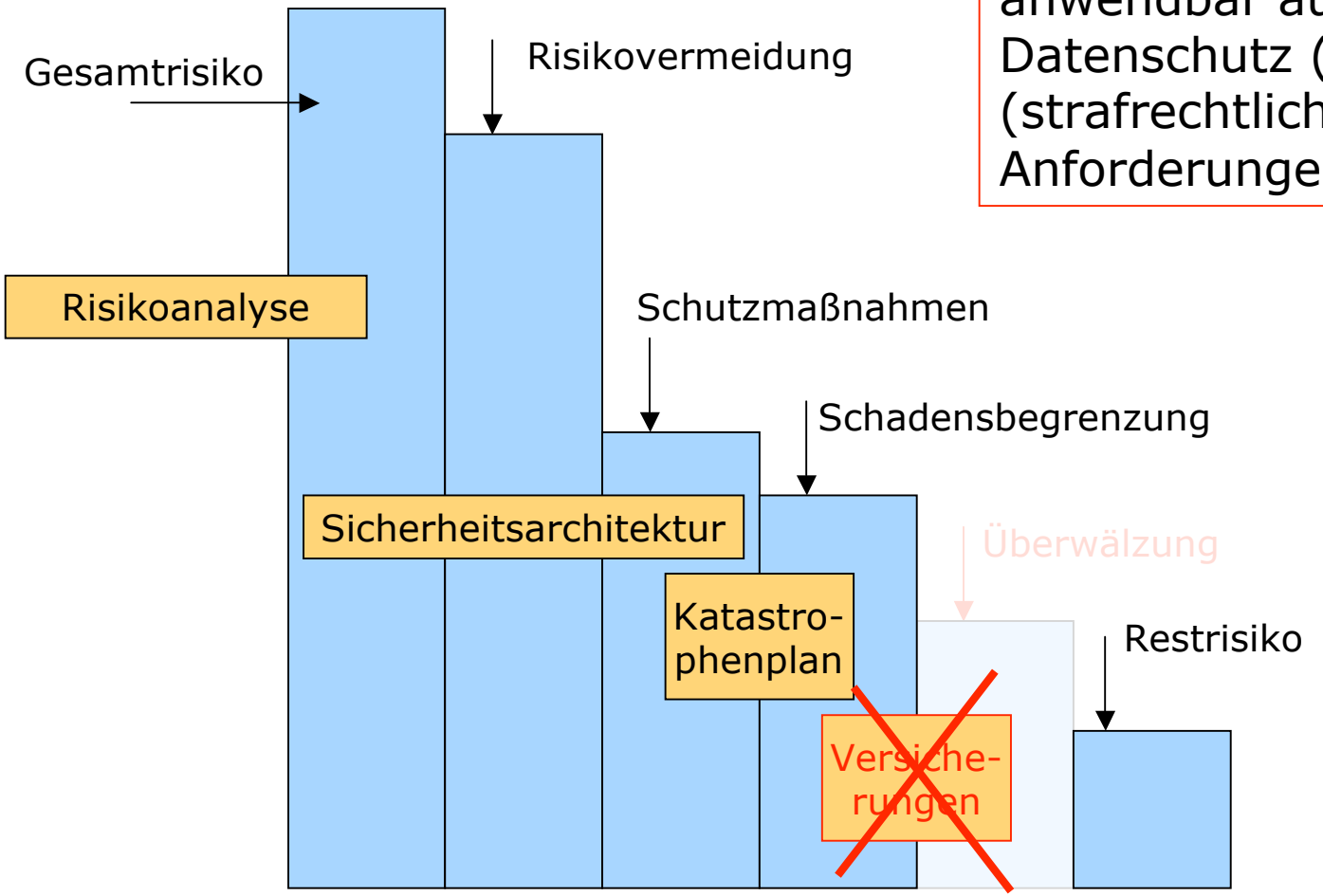
Risiko-Management für IT-Systeme



nach: Schaumüller-Bichl

Risiko-Management im Datenschutz

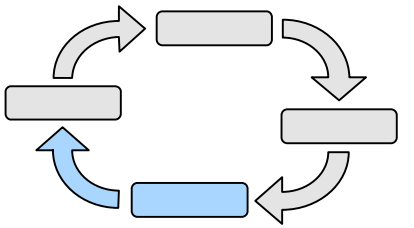
Überwälzung nicht anwendbar auf Datenschutz (und (strafrechtliche Anforderungen)



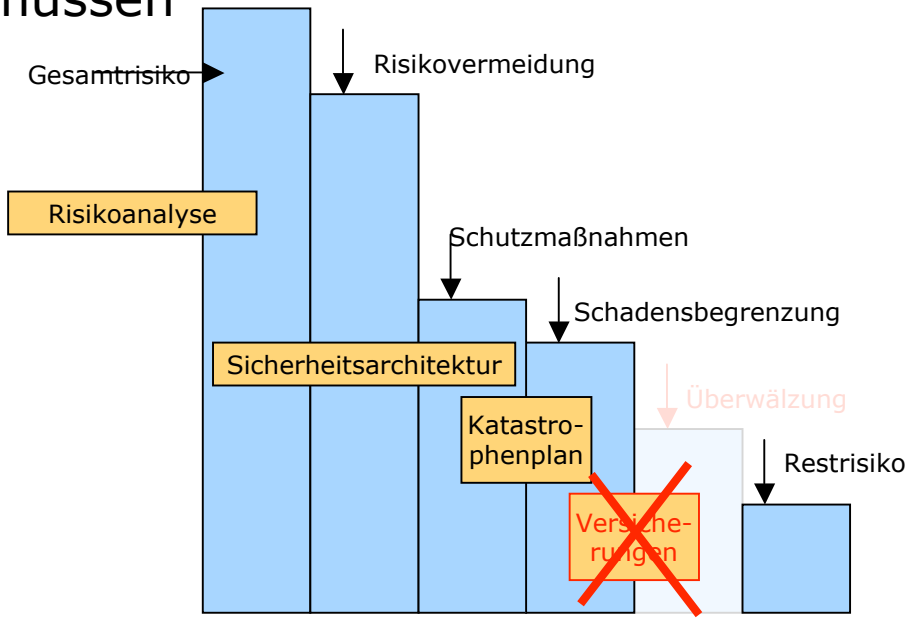
nach: Schaumüller-Bichl

Risiko-Management im Datenschutz

- IT-Sicherheit:
  - Risiko = Wahrscheinlichkeit · Schadenshöhe
  - Schäden sind systematisch tolerierbar

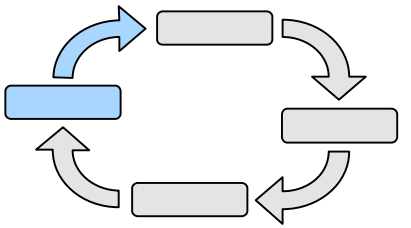


- Datenschutz:
  - Alles-Oder-Nichts-Ansatz
  - Rechtliche Vorgaben müssen umgesetzt werden

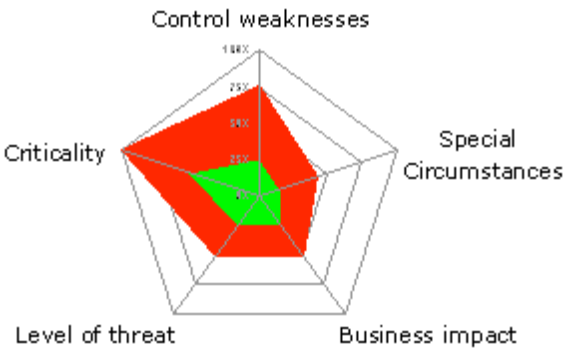


nach: Schaumüller-Bichl

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

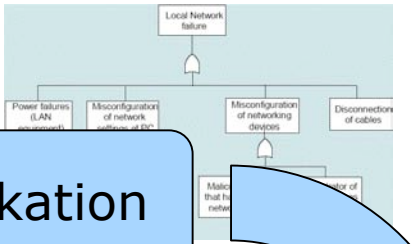


nach: Loomans, 2002

Risikomanagement Kreislauf

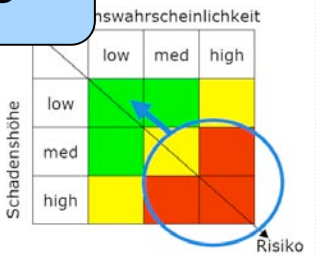
Checklisten
Workshops
Experten
Histor. Daten

Identifikation



Basisansatz
Kategorien
Quantitative
Verfahren

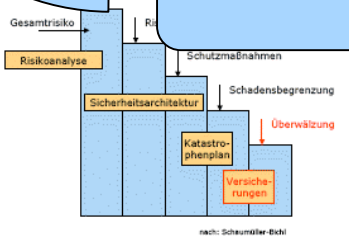
Bewertung



Risiko =
Eintrittswahrschein-
lichkeit · Schadenshöhe

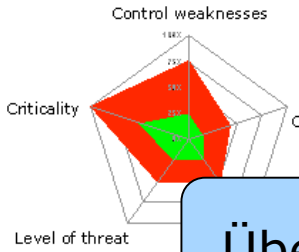
Best Practice
Scoring
Quant.
Verfahren

Steuerung



Checklisten
Scorecards
Kennzahlen

Überwachung



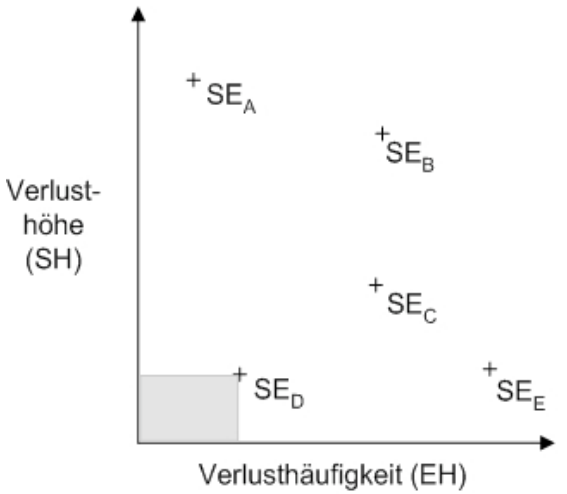
Risiko-Management für IT-Systeme

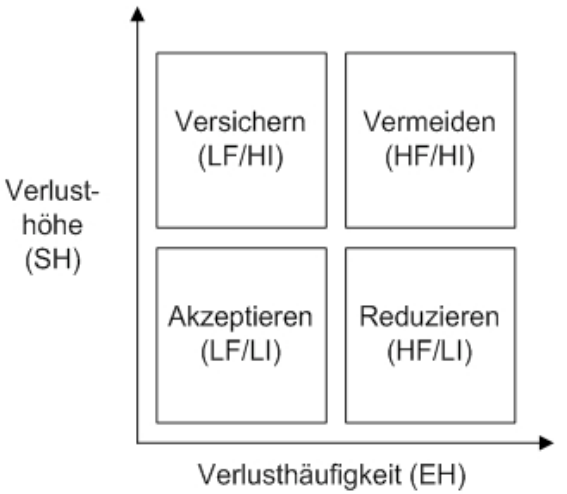
- IT-Sicherheitskonzept kann Risiko niemals 100-prozentig beseitigen
  --> Notfallplan zur Schadensbegrenzung
    - sollte Teil der Maßnahmenplanung sein
- Methoden
  - Back-Up-Planung (Rechenzentrum, Daten)
  - Notlaufkonzepte
  - Wiederbeschaffungs- und Wiederanlaufpläne
- Risiko-Management ist primär ausgerichtet auf die schnelle Beseitigung von Verlusten der Verfügbarkeit.
- Verlust von Vertraulichkeit
  - nahezu nicht umkehrbar, da Löschung aller Kopien kaum herbeiführbar
  - Schaden kann schleichend eintreten
- Verlust von Integrität
  - Schaden kann schleichend eintreten
  - schwer umkehrbar, Backup-Konzepte können helfen

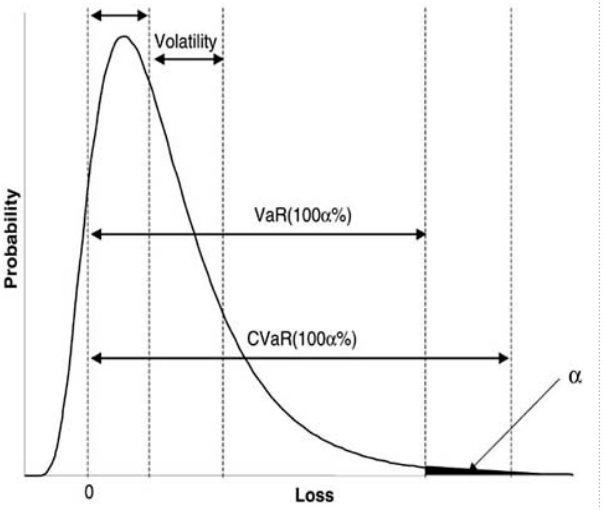
Quantitative Daten werden als Basis benötigt

- 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

Computer Crime and Security Surveys

- Herausgegeben vom U.S. Computer Security Institute CSI
  - http://www.gocsi.com/
  - bekannteste Langzeit-Umfrage zu IT-Sicherheitsvorfällen
- Stichprobe
  - über 500 IT-Sicherheitsspezialisten aus verschiedenen Branchen

Computer Crime and Security Surveys

- Hauptergebnisse (2003)
  - Schäden in Unternehmen
    - Hauptschäden entstehen durch Datendiebstahl
    - Zweite Stelle: Schäden durch Denial-of-Servcie-Angriffe
  - Angriffsarten
    - 82 Prozent Virenangriffe
    - 80 Prozent Datenmissbrauch durch Insider
  - Reaktion auf Angriffe
    - 93 Prozent schließen Sicherheitslöcher
    - 50 Prozent verheimlichen Sicherheitslöcher
    - 30 Prozent verfolgen Angreifer (law enforcement)

Computer Crime and Security Surveys

- Hauptergebnisse 2007
  - Anstieg der Verluste durch Sicherheitsprobleme von 168.000 Dollar (2006) auf 350.000 Dollar (2007)
    - höchster Wert seit 2004
    - 18 Prozent der Befragten waren Opfer eines gezielten Angriffs
  - Hauptursache von Verlusten
    - in den vergangenen sieben Jahren: Viren (Schadsoftware)
    - nun an erster Stelle: »Financial fraud«
  - Insider-Angriffe
    - 59 Prozent der Fälle: unerlaubte Netznutzung
    - 52 Prozent der Fälle: Verseuchung mit Viren

Gründe für mangelnde Informationssicherheit

Es fehlt an Geld	55 %
Es fehlt an Bewusstsein bei den Mitarbeitern	52 %
Es fehlt an Bewusstsein und Unterstützung im Topmanagement	45 %
Es fehlt an Bewusstsein und Unterstützung beim mittleren Management	37 %
Es fehlen verfügbare und kompetente Mitarbeiter	32 %
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	31 %
Es fehlen die strategischen Grundlagen/Gesamtkonzepte	29 %
Die Kontrolle und Einhaltung ist unzureichend	27 %
Anwendungen sind nicht für Informationssicherheitsmaßnahmen vorbereitet	25 %
Die vorhandenen Konzepte werden nicht umgesetzt	22 %
Es fehlen realisierbare (Teil)-Konzepte	19 %

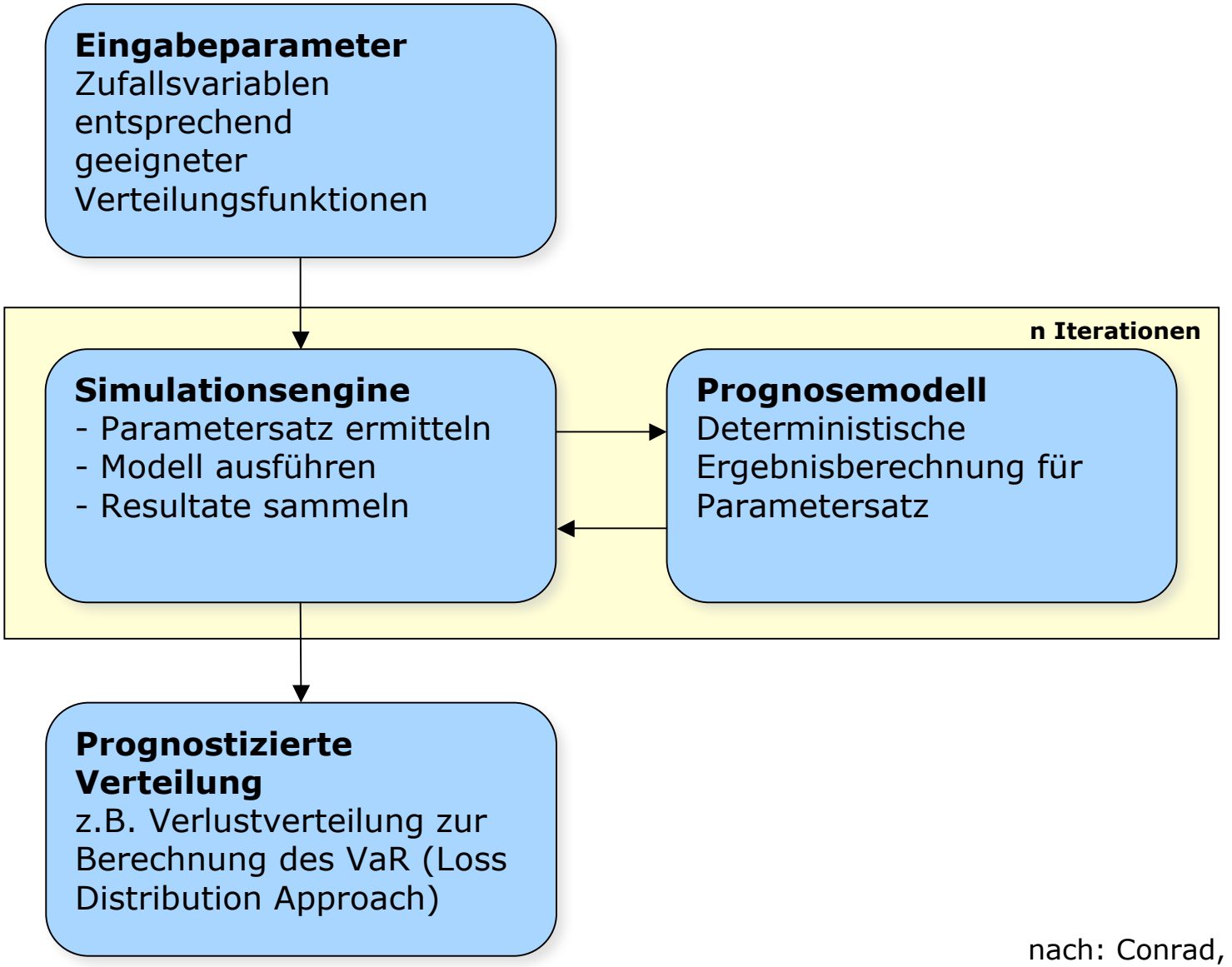
Basis: 158 Antworten

Quelle: <kes>/Microsoft-Sicherheitsstudie 2006
aus: ZIEL:SICHER 01/2007, Microsoft 2007, S. 6

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

Simulationen - Beispiel Monte Carlo Simulation



nach: Conrad, 2005

Simulationen - Beispiel Monte Carlo Simulation

- Grundprinzip
  - Risikoparameter werden als Zufallsparameter modelliert, z.B.
    - Auftretenshäufigkeit mit Poisson-Verteilung
    - Verlusthöhe mit Generalized Pareto Distribution (GPD)
  - Unsicherheit bezüglich der Eingabedaten lässt sich durch Zufallsverteilungen abbilden
  - Wiederholte Ausführung einer deterministischen Berechnung für verschiedene Werte der Zufallsvariablen
  - Sammlung der Resultate ergibt Verteilungsfunktion als Ergebnis

- Value at Risk (VaR) als typische ableitbare Kennzahl
  - Wie hoch ist der mögliche Verlust, der mit einer Wahrscheinlichkeit von x % nicht überschritten wird?

- Offenes Problem
  - Welche Verteilungsfunktionen (wie parametrisiert) bilden die Realität am besten ab?

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

Marktmechanismen - Beispiele

- Event Studies
  - Änderung des Börsenwerts eines Unternehmens nach dem Bekanntwerden eines Sicherheitsvorfalls
  - Untersuchung: Internet Sicherheitsvorfall führte zu 2,1 % durchschnittlichem Marktwertverlust (Cavusoglu et al. 2004)
- Bug Challenges/Bounties/Auctions (z.B. Schechter 2004)
  - Einfachster Fall: Hersteller bietet Prämie für das Brechen eines Algorithmus, Aufdecken einer Schwachstelle, etc.
- Exploit Derivate (z.B. Böhme 2006)
  - Ausgabe binärer Optionen
  - Teil 1: führt zu Auszahlung falls bis zum Termin eine Sicherheitslücke in System X gefunden wird.
  - Teil 2: führt zu Auszahlung im umgekehrten Fall

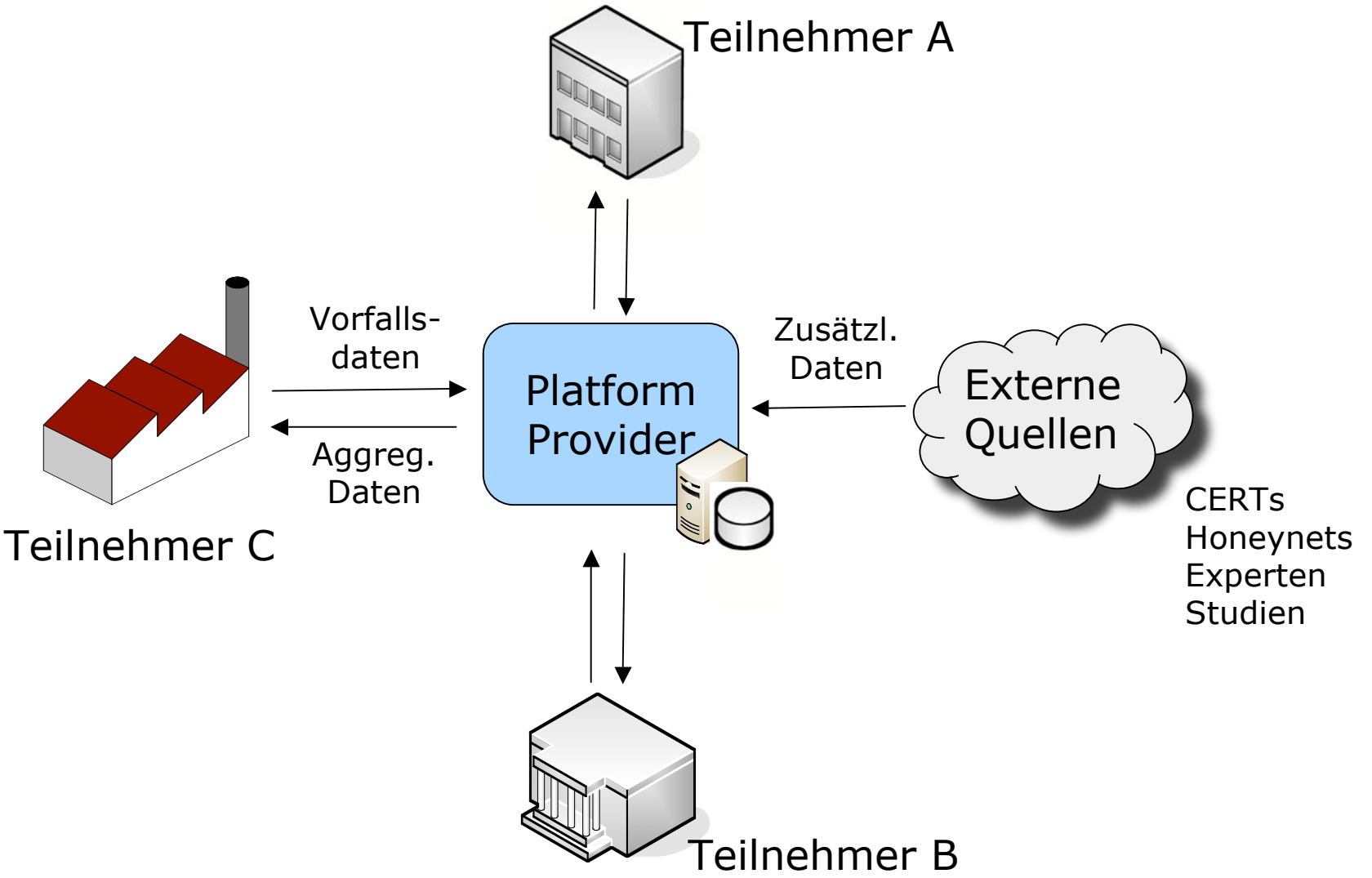
Mögliche Quellen für quantitative Daten

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

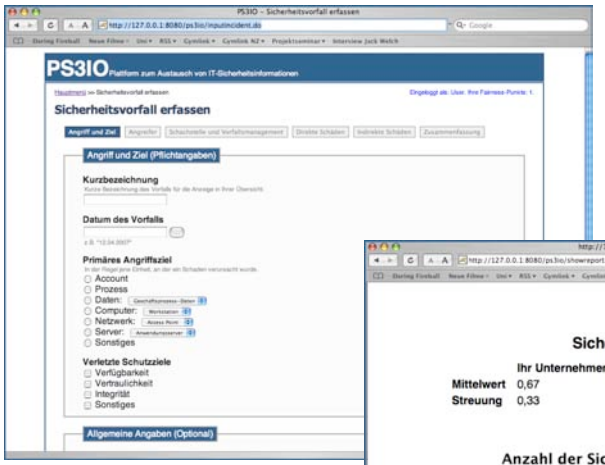
- Idee
  - Entwurf eines Systems zur Sammlung von quantitativen historischen Daten über Sicherheitsvorfälle in Organisationen.
- Ziel
  - Aufbau einer Datenbasis die Informationen über Schadenshöhe, Eintrittswahrscheinlichkeit und Wahrscheinlichkeitsverteilungen von Sicherheitsvorfällen in verschiedenen 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

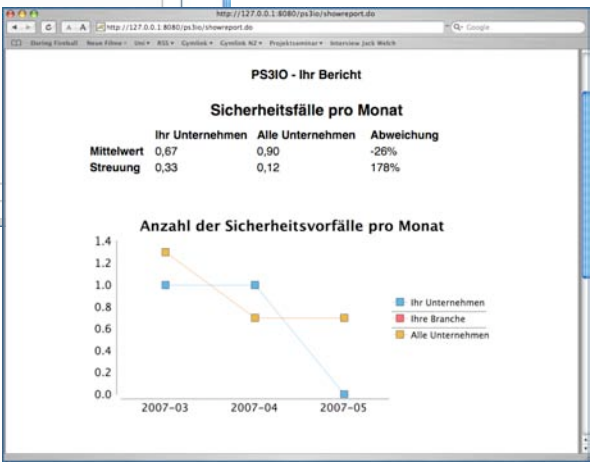
Basisarchitektur



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

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

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