T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2010

Köln, 03./04.11.2010

Dr. Thomas Nowey
Krones AG

Wirtschaftlichkeit der IT-Sicherheit

Produktionsstätten in Deutschland

Flensburg

Fertigung	Reinigungsmaschinen, Pasteure
Mitarbeiter	504*
erworben	1988

Nittenau

Fertigung	Großteile
Mitarbeiter	797*
gegründet	1972

Freising

Werk Steinecker

Fertigung	Brauerei-/Filteranlagen, Automation, Prozesstechnik
Mitarbeiter	457*
erworben	1994

Neutraubling

Hauptwerk	
Mitarbeiter	5,404*
gegründet	1951

Rosenheim

Fertigung	Verpackungsmaschinen
Mitarbeiter	892*
gegründet	1997

10,293 Mitarbeiter, weltweit
8,054 Mitarbeiter in Deutschland

* 30.06.2010

KRONES

krones Geschäftsbereiche

Anlagen-Kompetenz

Prozesstechnik


CSD


Wasser


Bier


Alkohol


Milchprodukte


Non-Food

Abfüll- und Verpackungstechnik

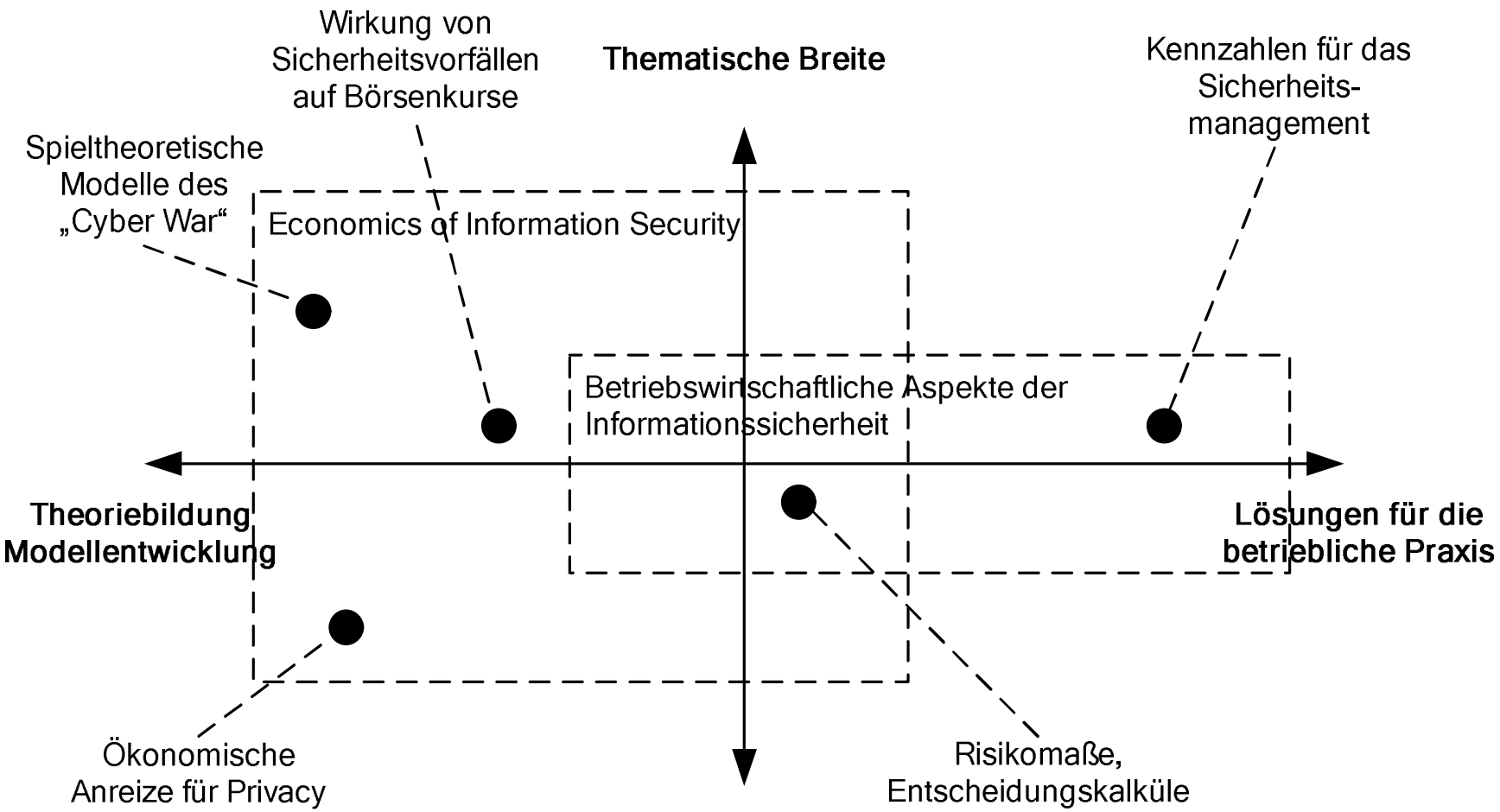
Kunststoff | Reinigung | Füllen | Inspizieren | Etikettieren | Transport | Packen

Intralogistik

IT-Lösungen

Lifecycle Service

Ökonomische Aspekte der Informationssicherheit



Geben wir zu viel oder zu wenig für IT-Sicherheit aus?

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

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

Sind IT-Sicherheitsmaßnahmen wirtschaftlich sinnvoll?

- **How much is enough?**
  (Kevin J. Soo Hoo, Dissertation, Stanford, 2000)

- **Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen?**
  (Pohlmann in HMD 248, 2006)

- **Wie viel darf IT-Sicherheit kosten?**
  (Weidenhammer, GAI NetConsult, 2003)

- **Finally a Real Return on Security Spending**
  (Scott Berinato im CIO Magazine 2002)

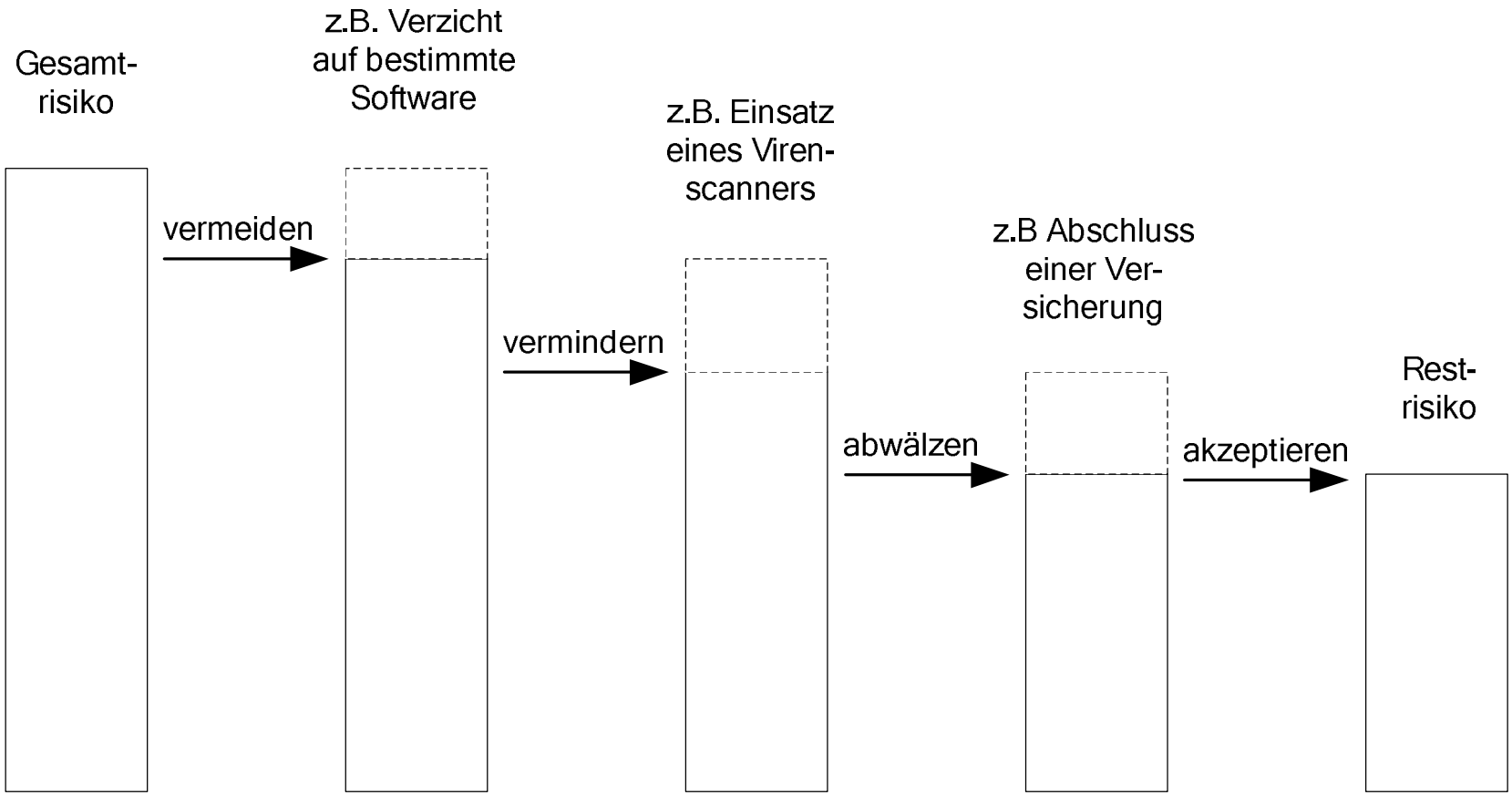
Wann werden Wirtschaftlichkeitsaussagen benötigt?

- Planung (ex ante)
  - Festlegung von Budgetforderungen für IT-Sicherheit
  - Festlegung von Budgets für IT-Sicherheit
  - Entscheidung über die Behandlung von Risiken
  - Umgang mit plötzlich auftretenden neuen Gefährdungen
  - Entscheidung für oder gegen eine spezifische Sicherheitsmaßnahme
  - Auswahl des richtigen Bündels an Sicherheitsmaßnahmen

- Überprüfung (ex post)
  - Überprüfung des Budgets für IT-Sicherheit
  - Überprüfung der Effektivität und Effizienz von Maßnahmen
  - Vergleich zwischen Unternehmensbereichen/Investitionsobjekten
  - Vergleich mit anderen Unternehmen/Benchmarking

Sicherheitsmanagement ist Risikomanagement

Risikosteuerung als zentraler Bestandteil des Sicherheitsmanagements



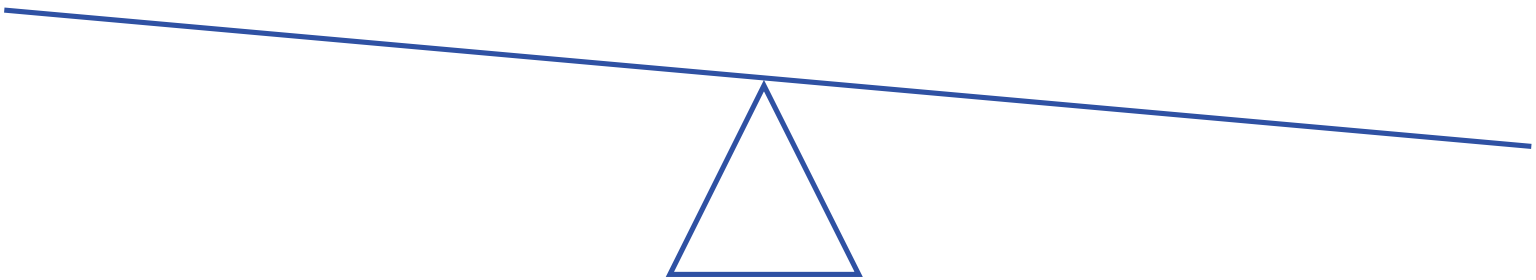
Kosten und Nutzen von Sicherheitsmaßnahmen

Kosten

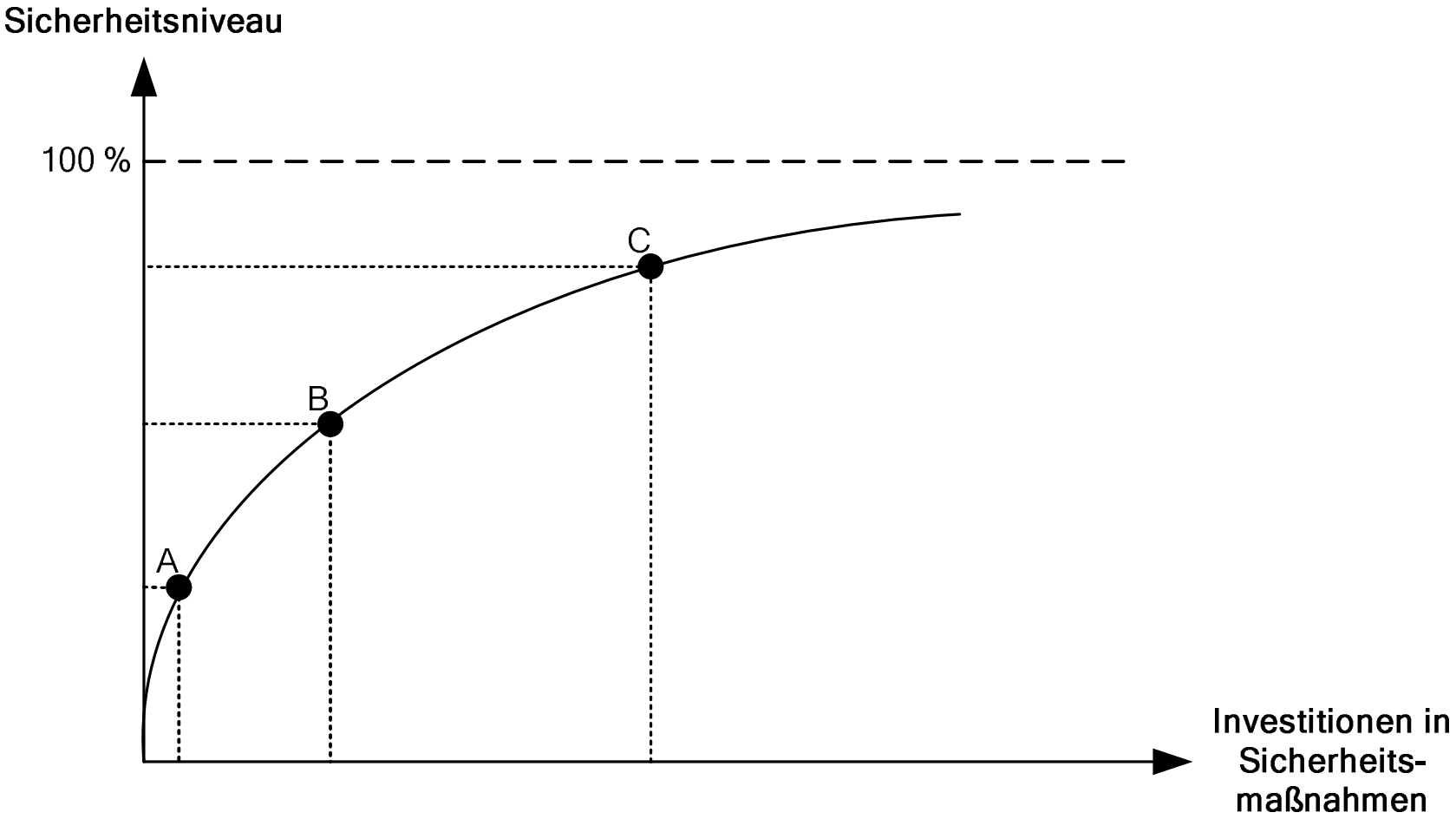
- Anschaffungskosten
- Einrichtungskosten
- Betriebskosten
- Kosten durch Veränderung betrieblicher Abläufe

Nutzen

- Reduktion der Häufigkeit von Sicherheitsvorfällen
- Reduktion der Schwere von Sicherheitsvorfällen
- Eröffnung neuer Geschäftsmöglichkeiten
- Vereinfachung von betrieblichen Abläufen

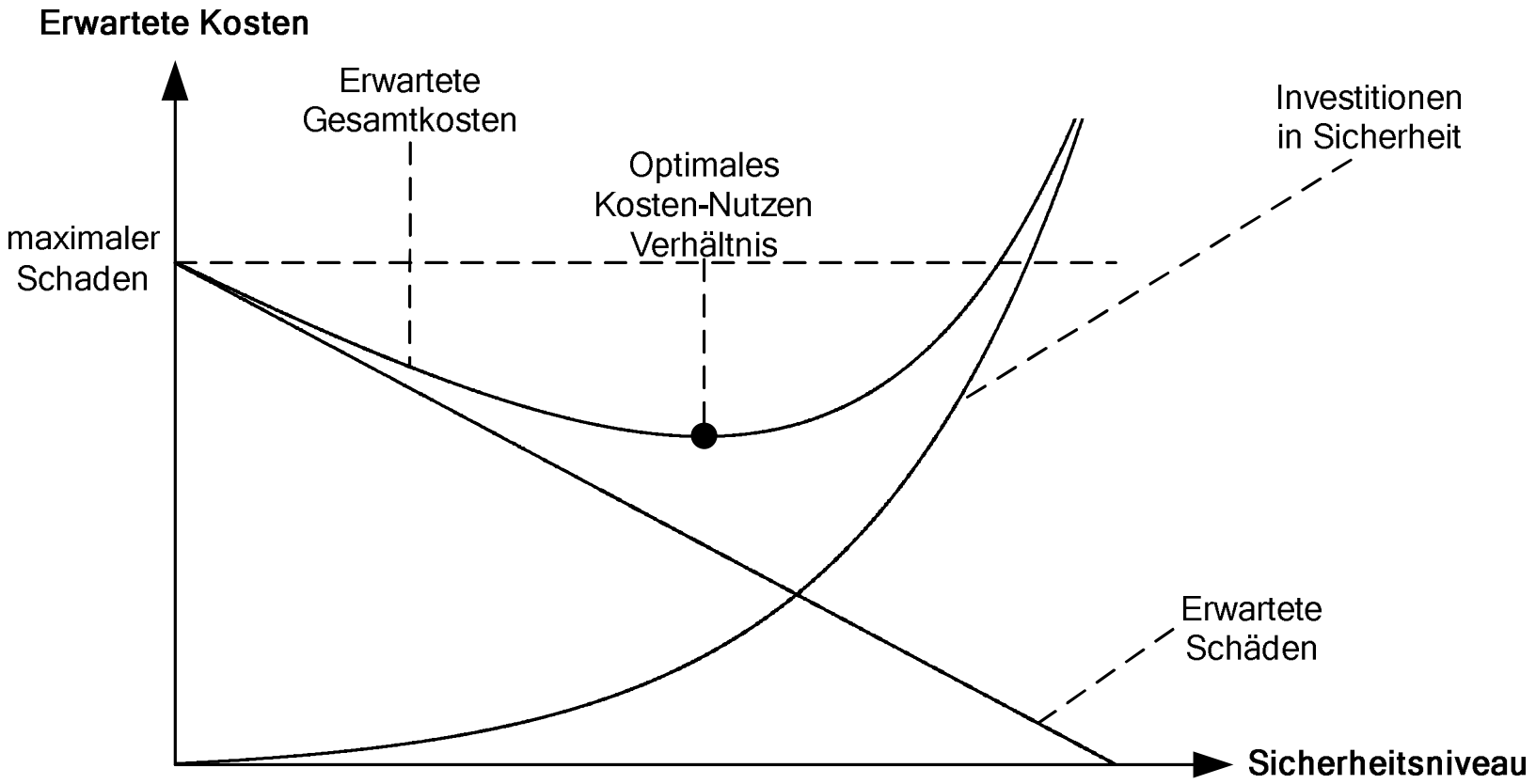


Abnehmender Grenznutzen



Quelle: BSI 100-2

Kosten-Nutzen-Verhältnis



Konzepte für das Risikomanagement

	Best Practice	**Qualitativ**	**Quantitativ**
Identifikation	Gefährdungskatalog	Expertenbefragung, Kreativitätstechniken	Analytische Verfahren, vergangene Vorfälle
Bewertung	Für alle gleich, Implizit durch Aufnahme in Katalog	Individuelle, ordinalskalierte Bewertung	Individuelle, verhältnisskalierte Bewertung
Steuerung	Implizit durch Maßnahmenkataloge	Nutzwertanalyse, Scoring-Modell	Quantitatives Entscheidungskalkül wie VaR
Überwachung	Review durch Experten, Überarbeitung der Kataloge	Indikatoren, Scorecards	Metriken, Kennzahlen

Risikomaße – Beispiel ALE (Annual Loss Expectancy)

Annual Loss Expectancy (ALE) nach Soo-Hoo, 2000

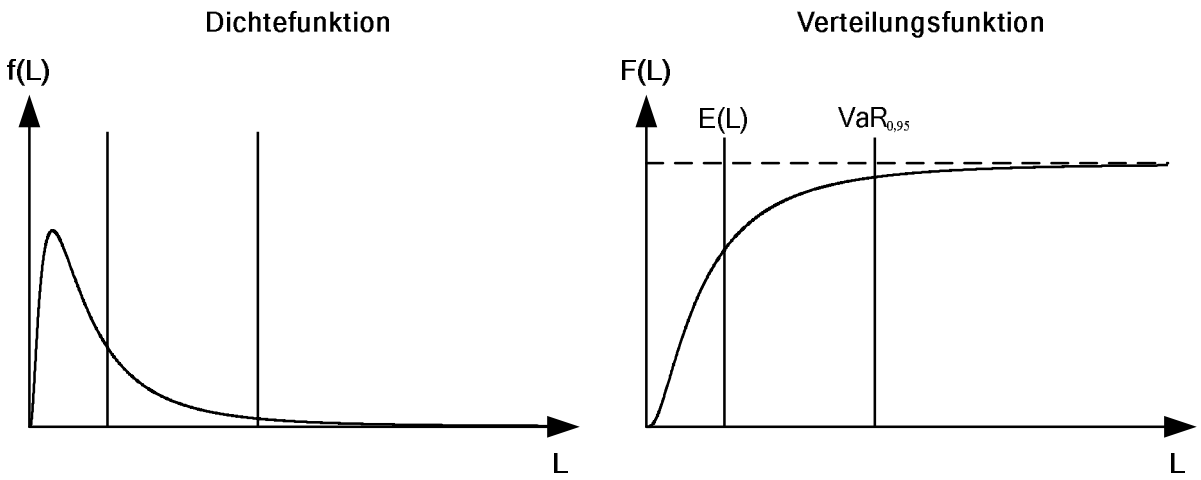
$$ALE = \sum_{i=1}^{N} I(O_i) \cdot F_i$$

mit

ALE = jährliche Verlusterwartung

$I(O_i)$ = Schadenshöhe bei Ereignis i

F_i = Häufigkeit von Ereignis i



Entscheidungsregeln – Beispiele ROSI und NKW

Return on Security Investment (ROSI) nach Wei et al., 2001 und Pfleeger et al., 2003

$$ROSI_1(\text{klassisch}) = ALE_{\text{ohne Maßnahme}} - ALE_{\text{mit Maßnahme}} - Kosten_{\text{Maßnahme}}$$

$$ROSI_2(\text{ROI}-\text{ähnlich}) = \frac{ALE_{\text{ohne Maßnahme}} - ALE_{\text{mit Maßnahme}}}{Kosten_{\text{Maßnahme}}}$$

Nettokapitalwert-basierte Betrachtung (NKW) nach Faisst et al., 2007

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

mit

I_0 = Anfangsinvestition für Sicherheitsmaßnahme

$\Delta E(L_t)$ = Reduktion des erwarteten Schadens in t

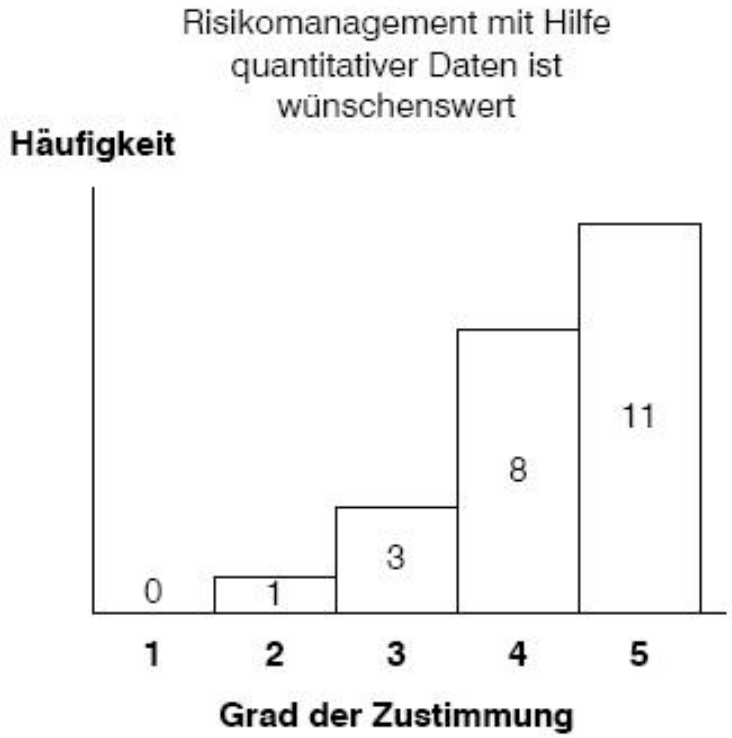
ΔOCC_t = Reduktion der Opportunitätskosten in t

C_t = Kosten für Sicherheitsmaßnahme in t

i_{calc} = Kalkulationszinssatz

KRONES

Ergebnisse einer Expertenstudie



Voraussetzungen für Wirtschaftlichkeitsbetrachtungen

- Risikoorientierter, ganzheitlicher Ansatz zum Management von Informationssicherheit
  - Assets, Risikomanagementprozess, Incident Handling Prozess

- Festlegung der Ziele
- Festlegung der Risikopolitik

- Klare Definition von Kosten für Informationssicherheit
- Klare Definition von Informationssicherheitsrisiken und zusätzlicher Nutzenfaktoren

- Abstimmung mit anderen Unternehmensbereichen (z.B. ERM)

- Auswahl eines Risikomaßes (z.B. ALE)
- Auswahl einer Entscheidungsregel (z.B. ROSI)
- Festlegung der Datenquellen und des Weges zur Ermittlung der relevanten Größen
- Festlegung der Dokumentation und des Reportings

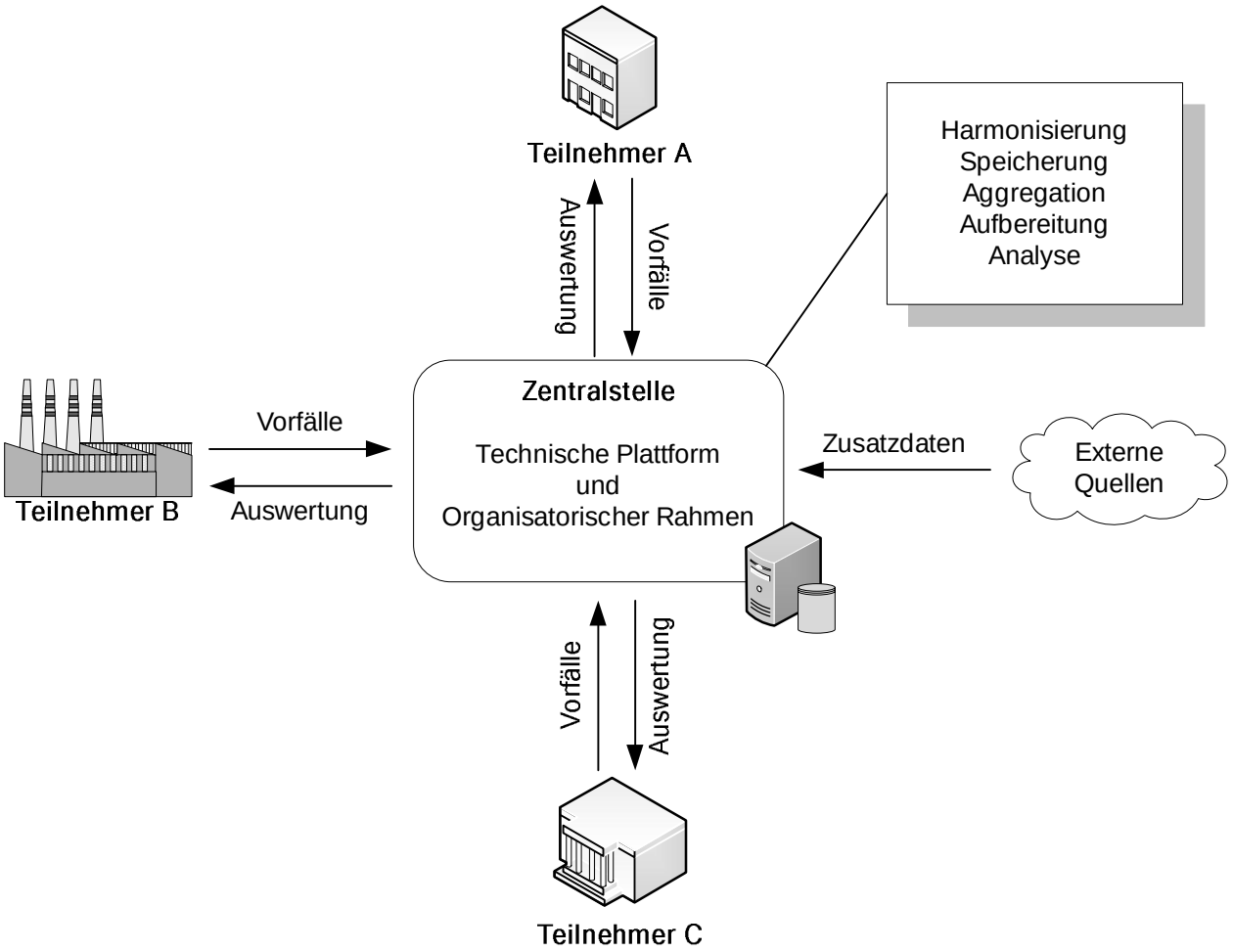
Bewertung des (potentiellen) Schadens durch Sicherheitsvorfälle

Schadensart	Metrik
Vorfallsbehandlung und Wiederherstellung	Wiederbeschaffungskosten (€) Arbeitszeit (Personentage)
Beeinträchtigung betrieblicher Prozesse	Dauer (Zeiteinheiten) Entgangener Gewinn (€)
Finanzieller Schaden	Verlust (€)
Verlust sensibler Daten	Entstandener Nachteil/Wert (€)
Strafen/rechtliche Konsequenzen	Strafrechtliche Konsequenzen Vertragsstrafen/Bußgelder (€)
Negative Außenwirkung	Bewerteter Imageschaden (€)
Personenschaden	Anzahl der Betroffenen Schwere des Schadens
Sonstiger Schaden	Schätzung (€)

➔ **Die Bewertung kann nicht alleine durch die IT erfolgen**

KRONES

Ein Konzept zum überbetrieblichen Austausch



Fazit

- These 1: Die Beschäftigung mit wirtschaftlichen Aspekten der IT-Sicherheit ist unausweichlich
- These 2: Wirtschaftlichkeitsbetrachtungen erfordern einen Risikomanagementansatz
- These 3: Echte Kosten-Nutzen-Betrachtungen erfordern quantitative Daten
- These 4: Die Formeln kommen zum Schluss
- These 5: Ein zentraler Baustein ist die quantitative Bewertung vergangener Schadensereignisse
- These 6: Der Weg ist das Ziel
  - Wechselseitiges Verständnis für Herausforderungen bei allen Stakeholdern
  - Einfach starten und Komplexität steigern

Informationssicherheit ist ein kontinuierlicher Verbesserungsprozess

Vielen Dank!
Kontakt: thomas.nowey@krones.com

KRONES