SIEMENS

Information
and Communication
Networks

Bewertung von IT-Risiken

Prof. Dr. Jörg Sauerbrey
Siemens AG

Das IT-Sicherheits-Dilemma

SIEMENS

- Die **Mega-Trends** (Internet, E-Business und Mobilität) sind für Unternehmen lebenswichtig, werfen aber IT-Sicherheitsprobleme auf
- **Geschäftspartner** verlangen in zunehmenden Maße **IT-Sicherheit**
- Nur der Einsatz einzelner **Sicherheitsprodukte** bringt nicht zwangsläufig die **notwendige Sicherheit**
- Die Gewährleistung von IT-Sicherheit ist ein zunehmend **komplexer** werdender Prozess
- Sicherheit kostet Geld

Dieses Dilemma fordert fundierte Bewertung von IT-Risiken unter Berücksichtigung wirtschaftlicher Aspekte (Risikomanagement)

SIEMENS

Was ist ein IT-Risiko ?

Definition

Das Risiko ist das Produkt aus

- der **Eintrittswahrscheinlichkeit** einer Bedrohung mit
- dem **Wert** des zu schützenden Gutes

- **Beispiel** (allgemein)

  Eine Bank mit einem vorhandenen Bargeldbestand **(Wert)** unterliegt der Bedrohung ausgeraubt zu werden. Ein erhöhtes Risiko besteht, wenn diese Bedrohung über ein nicht vergittertes Rückfenster wahrscheinlicher wird **(Eintrittswahrscheinlichkeit)**

- **Beispiel** (IT)

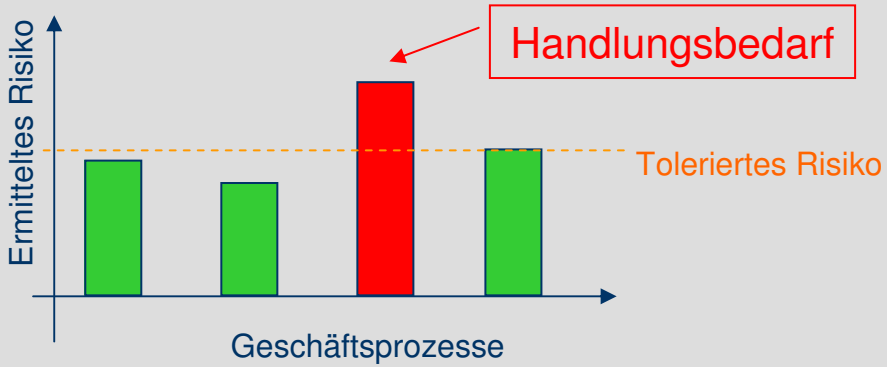
  Vertrauliche Daten **(Wert)** unterliegen der Bedrohung, unberechtig gelesen zu werden. Ein erhöhtes Risiko besteht, wenn diese Bedrohung über ein schwaches Passwort wahrscheinlicher wird **(Eintrittswahrscheinlichkeit)**

SIEMENS

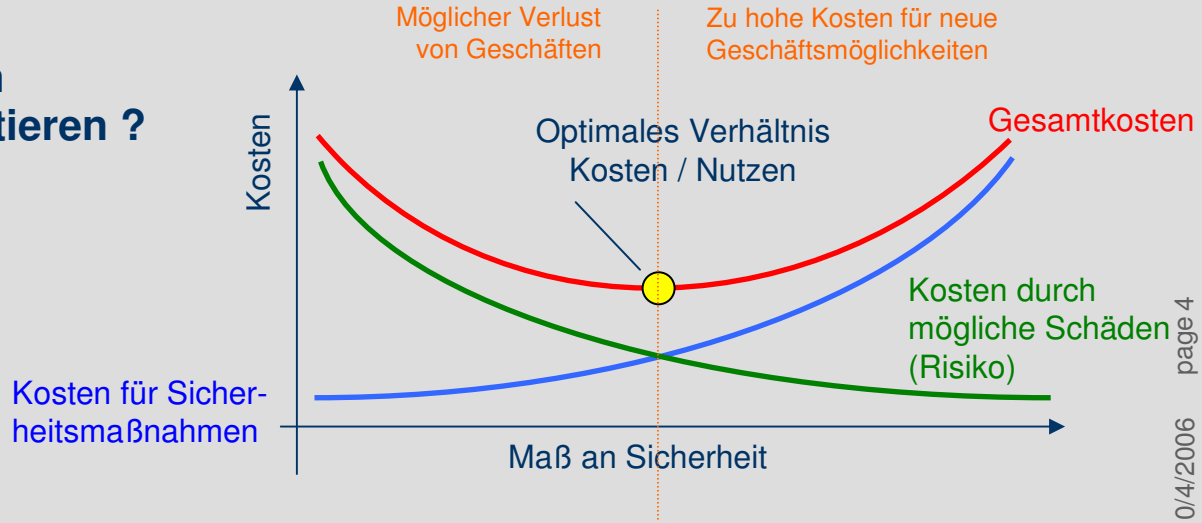
Wichtige Fragen beim Risikomanagement

Wo sollte ich investieren ?

(Welche Maßnahmen in welcher Reihenfolge)



Wieviel sollte ich insgesamt investieren ?



SIEMENS

Risikomanagement als Teil des Strategieprozesses

Jährliches Review ...

... Anpassen an die neue Situation

1. Schritt Strategie

2. Schritt Risikoanalyse und -bewertung

3. Schritt Auswahl

4. Schritt Umsetzung

Maßnahmenhandling

- Wo stehe ich heute?
- Wo will ich hin?
  - **neue Marktsegmente**
  - **Kundenbindung** erhöhen
  - **neue Produkte**/ Services
  - **neue Vertriebswege**
  - ...

- Welche **Geschäfts-prozesse** sind wichtig?
- Welches sind die unterstützenden **IT-Prozesse**/ - Komponenten?
- Welche **Risiken** bestehen?
- Welche **Maßnahmen** werden empfohlen?

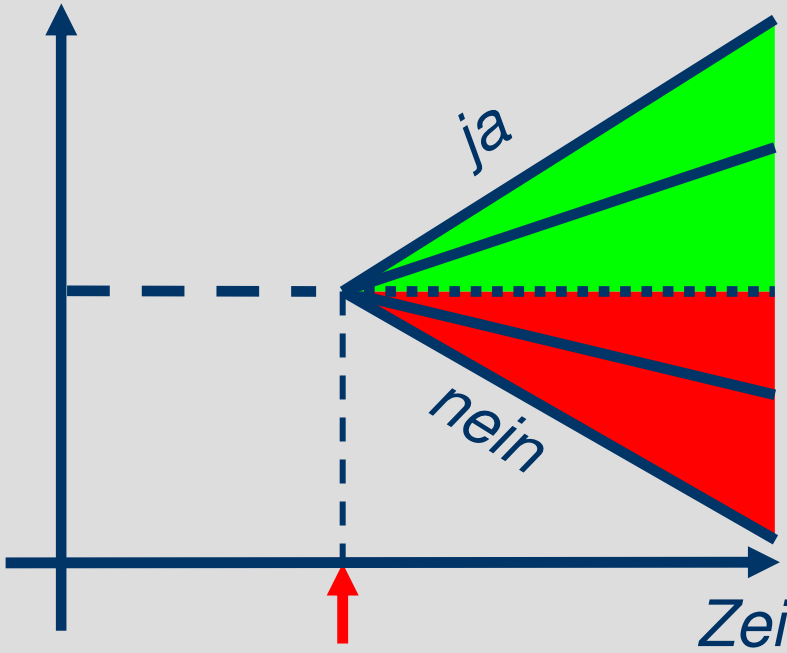
- Welche **Lösung** brauche ich?
- Welche **Komponenten** sind geeignet?
- Wie hoch sind die **Kosten**? (RoSI?)
- Wie soll die **Umsetzung** erfolgen?
- Wer ist der geeignete **Partner** ?

- **Regelwerk**
- **Implementierung** der Lösungen
- **Integration** in existierende Geschäftsprozesse
- **Betrieb**
- **Schulung** der Mitarbeiter
- **Controlling** der Lösungen

Geschäftlicher Nutzen (Return in Security Investment)

SIEMENS

Geschäftsergebnis
(= Umsatz – Kosten)



Investition in eine Security-Lösung

Umsatzsteigerung

- Zusatzgeschäft, z.B. durch sicheres E-Business
- Sicherer Zugriff von Außendienstmitarbeitern auf zentrale Daten (z.B. Angebotserstellung)

Kostensenkung

- Managed Security Services (Outsourcing)
- Verringerung Kommunikationskosten
- Prozessoptimierung

Kostenerhöhung

- Wiederherstellungskosten
- Höhere Versicherungsprämien

Umsatzausfall

- Denial of Service Angriffe

RoSI: Return on Security Investment

Risikoanalyse
Theoretischer Idealfall

SIEMENS

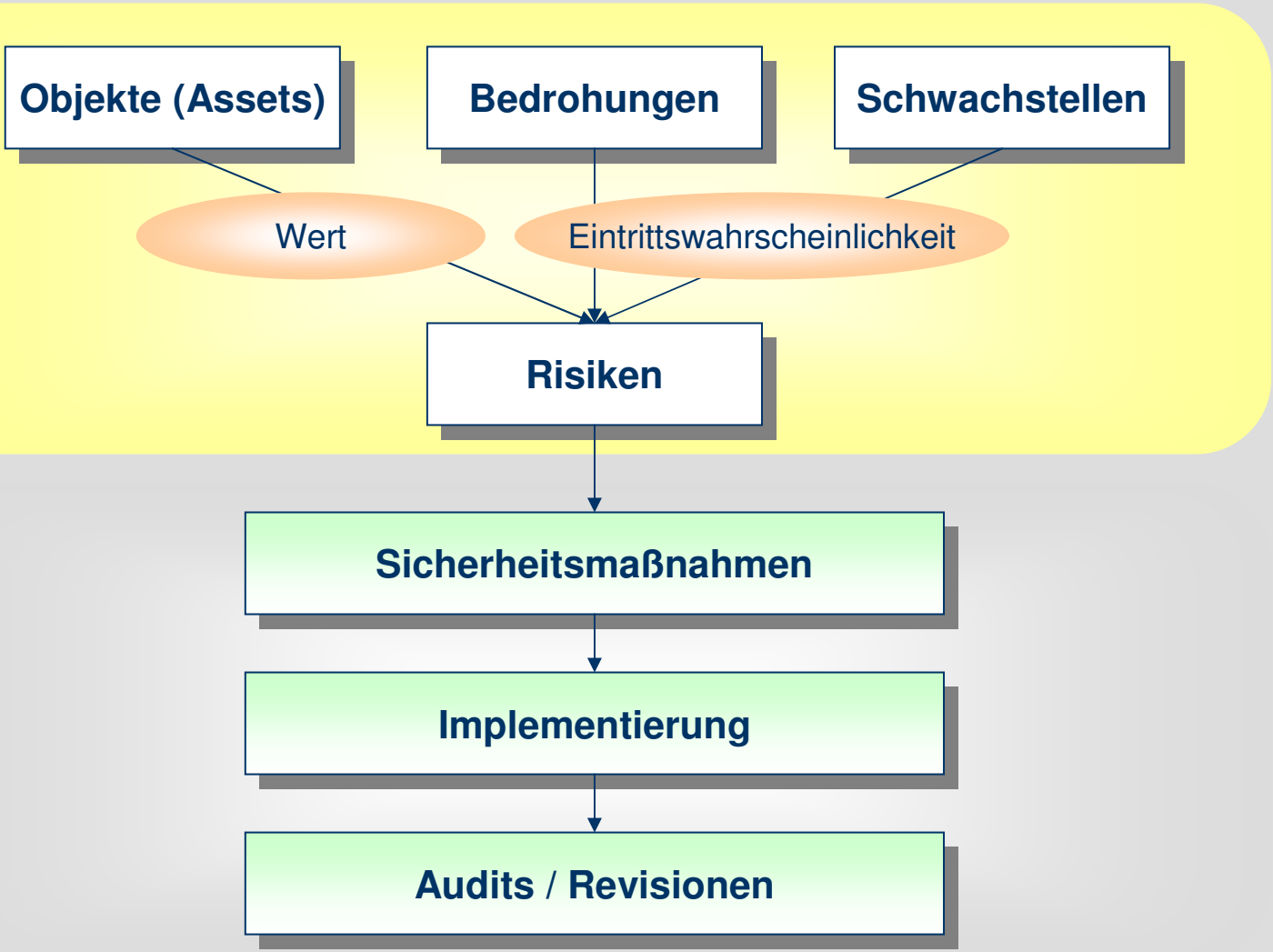
Risikomanagement

SIEMENS

Risikomanagement

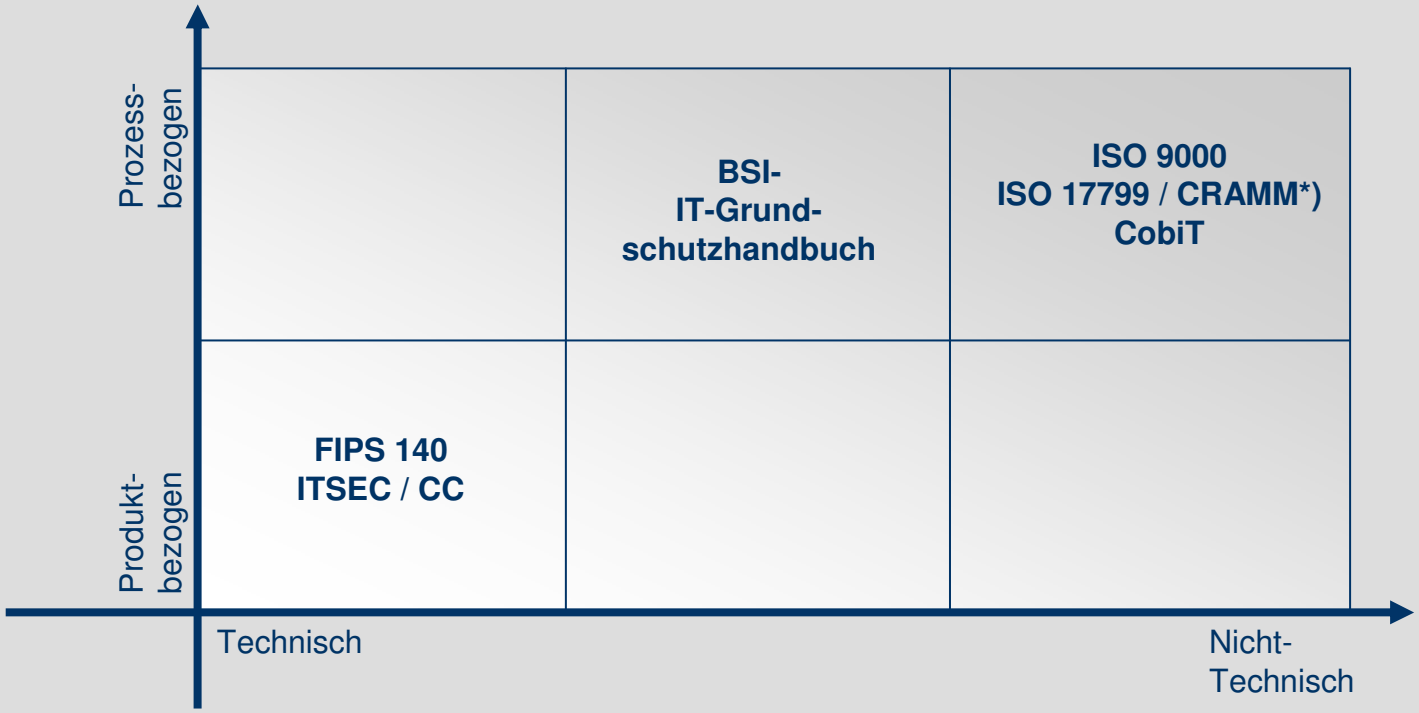
Risikoanalyse und –bewertung

Maßnahmen-handling



Risikomanagement: Standards / Methoden
Positionierung

SIEMENS



*) CRAMM: Methode / Tool um die Anforderungen aus dem BS7799 / ISO17799 programmgestützt erfüllen zu können

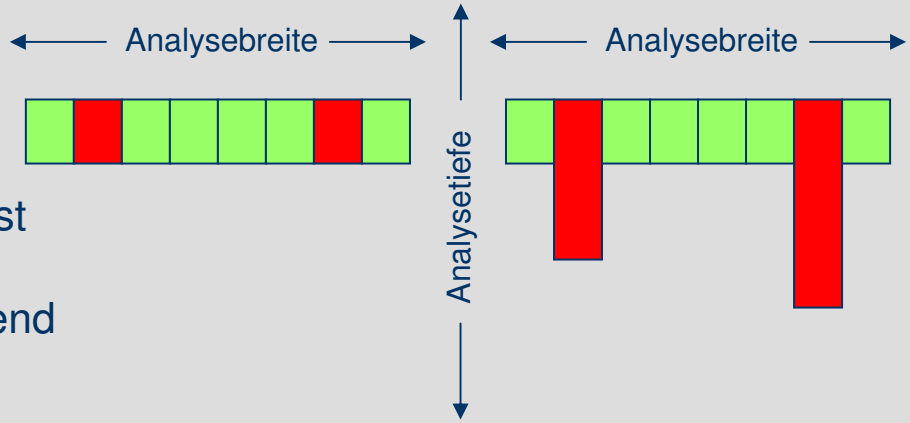
Quelle: Initi@tive D21

Gegenüberstellung von prozessbezogenen Standards / Methoden

SIEMENS

	Nicht-technisch z.B.: ISO17799 / CRAMM	Technisch z.B.: BSI IT-GS-Handbuch
Kostenaufwand	*niedrig*	*mittel*
Zeitaufwand	*niedrig*	*mittel*
Untersuchungstiefe	*flach*	*tief*
Anwendbarkeit der Methode	*einfach*	*einfach*
Tool-Unterstützung	*gut*	*gut*

Der Idealweg ist die Kombination aus beiden Vorgehensweisen. Zuerst den Handlungsbedarf ermitteln und anschließend tiefgreifend analysieren.



SIEMENS

Problempunkte und praktische Umsetzung

- Problempunkte der Risikobetrachtung
  - Keine 100% Sicherheit
  - Hoher Kosten- und Zeitaufwand für die Risikoanalyse
  - Sicherheit wird oft als hinderlich empfunden
  - Aufwand amortisiert sich nur indirekt
  - Verantwortlichkeiten oft nicht definiert / kommuniziert

- Faktoren für erfolgreiche, praktische Umsetzung der Methoden
  - Fundierte Planung und Budgetierung
  - Schrittweises Vorgehen, anstatt alles auf einmal
  - Strategisches Vorgehen, anstatt ereignisgesteuertem (bedarfs- bzw. mediengesteuertem) Aktionismus
  - Rechtzeitige Schulung von Management und Mitarbeitern (Awareness der Mitarbeiter für Sicherheit notwendig)
  - Kompetente Teams (evtl. Outsourcing) zur Umsetzung der Sicherheitsmaßnahmen
  - Controlling

Trends

SIEMENS

- Sichere Produkte allein sind nicht zwingend gleichzusetzen mit der Sicherheit eines Prozesses
- Die Prozess-orientierte Betrachtungsweise steht im Vordergrund
- Erhöhung von Transparenz und Verständlichkeit der Tools
- High-Level Ansatz, detaillierte Vertiefung nur da, wo Bedarf erkannt wurde
- Outsourcing aufgrund von Know-How- und Kapazitätsengpässen
- Stützen auf international anerkannte Standards
- Zertifizierungen als Wettbewerbsvorteil