



Institut für Business  
Consulting e.V.  
Furtwangen

IT-Grundschatz Audits

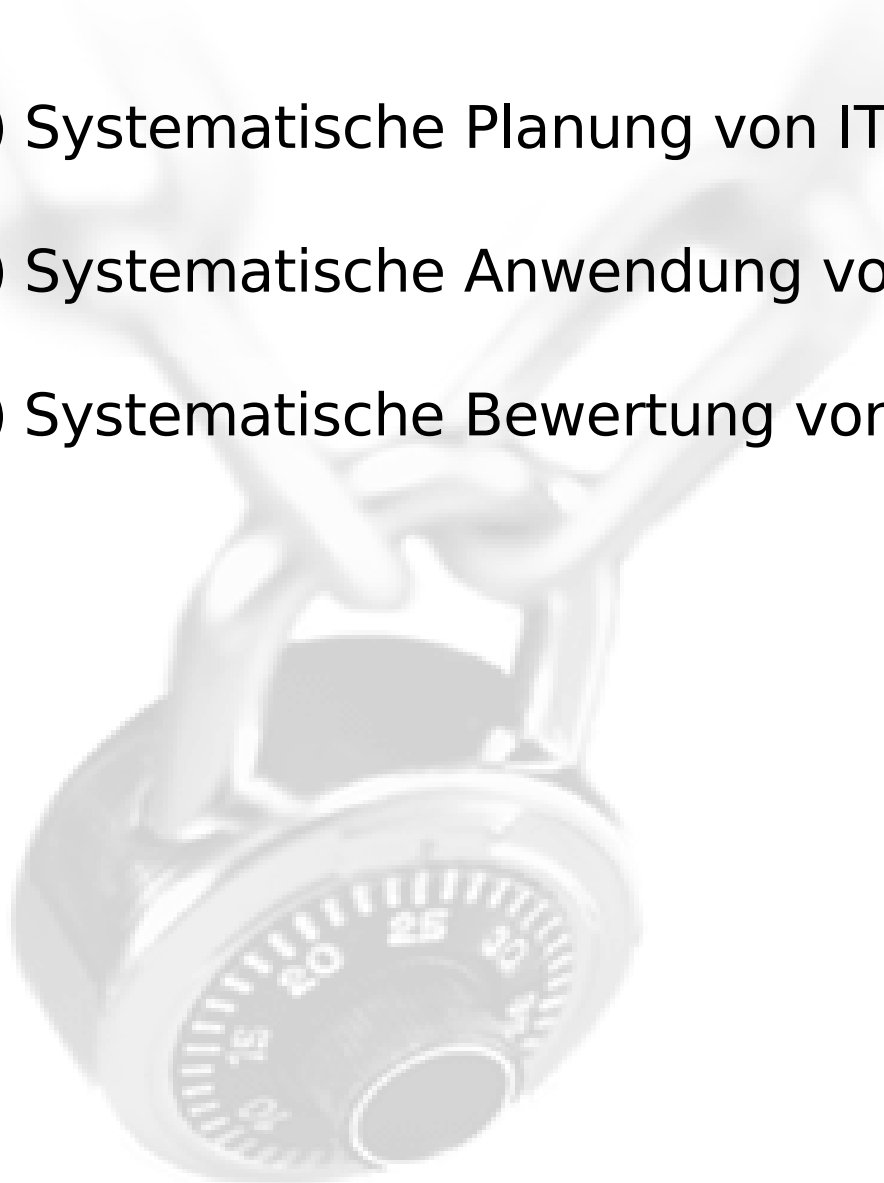


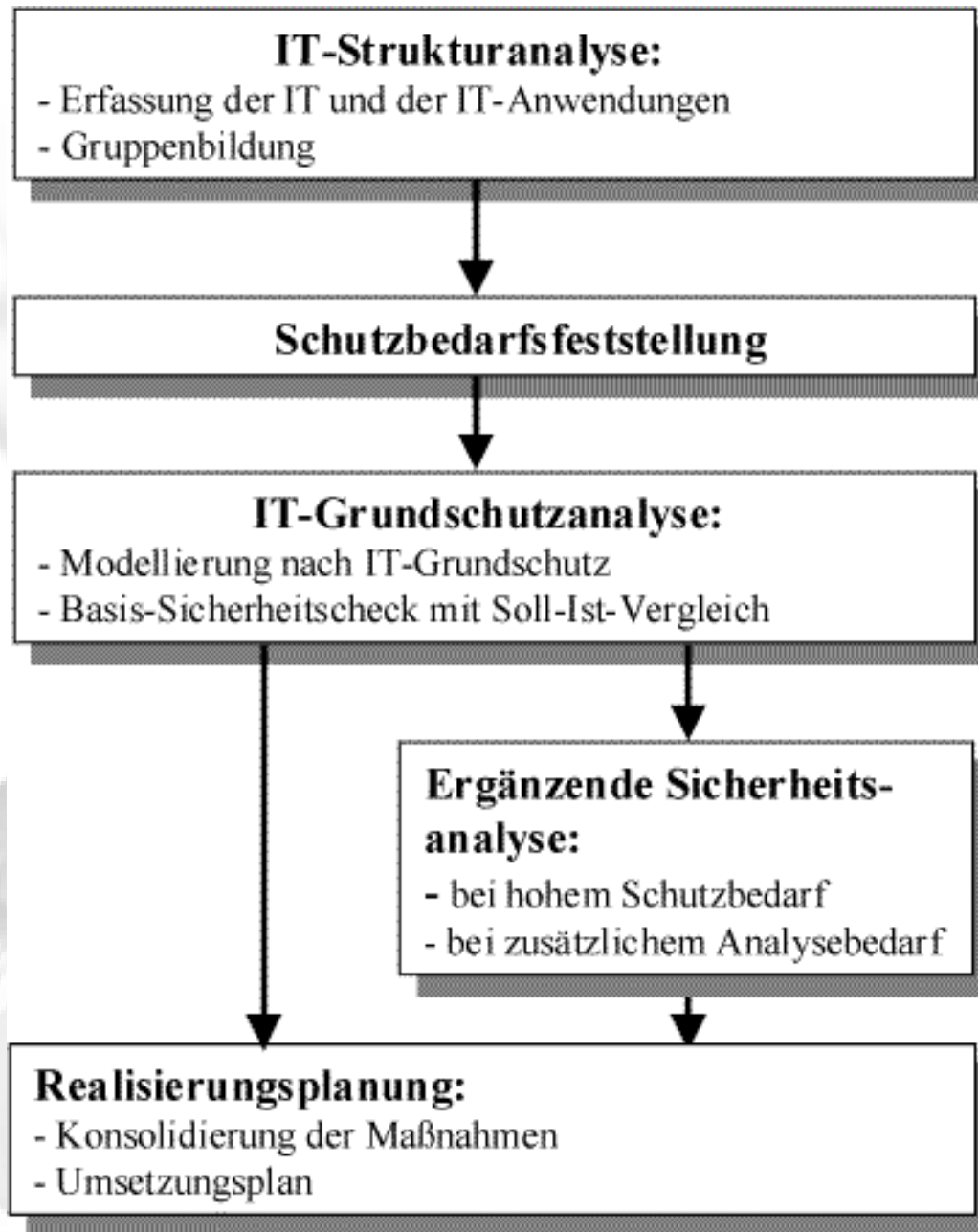


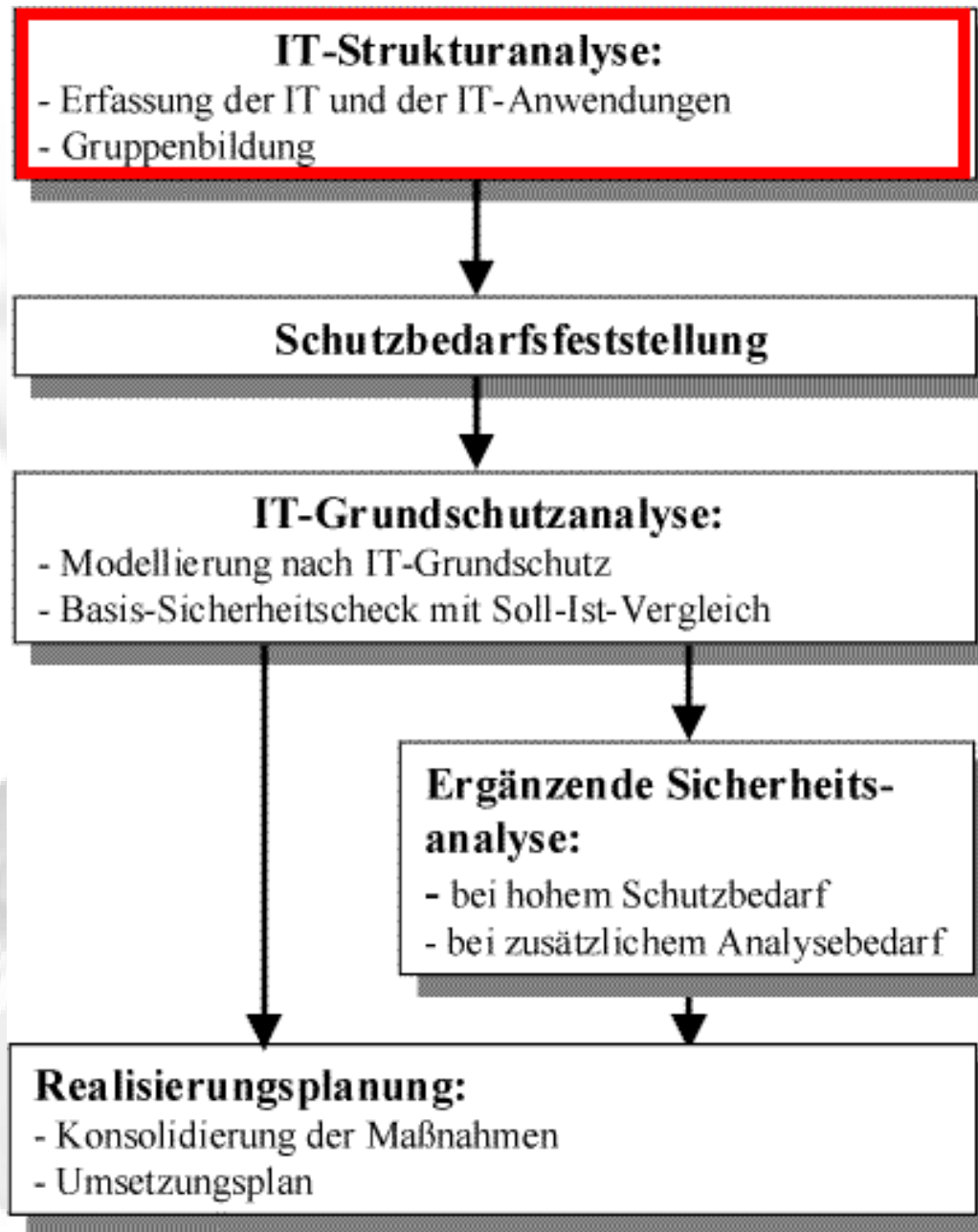
- Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik
- Klar gegliederte Sammlung von praxisnahen IT-Sicherheitsmaßnahmen
- Darlegung von Wechselwirkungen
- Festgehalten im IT-Grundschutzhandbuch



- (1) Systematische Planung von IT-Sicherheit
- (2) Systematische Anwendung von IT-Sicherheit
- (3) Systematische Bewertung von IT-Sicherheit



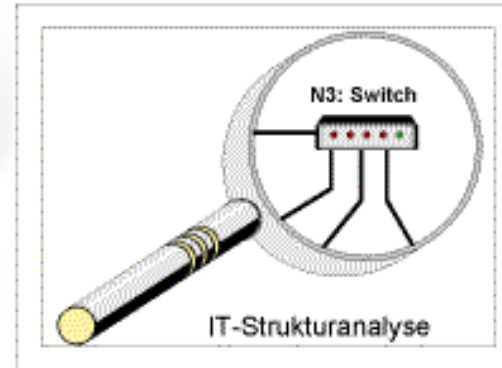






Basis: Netzplan (z.B. Netztopologie)

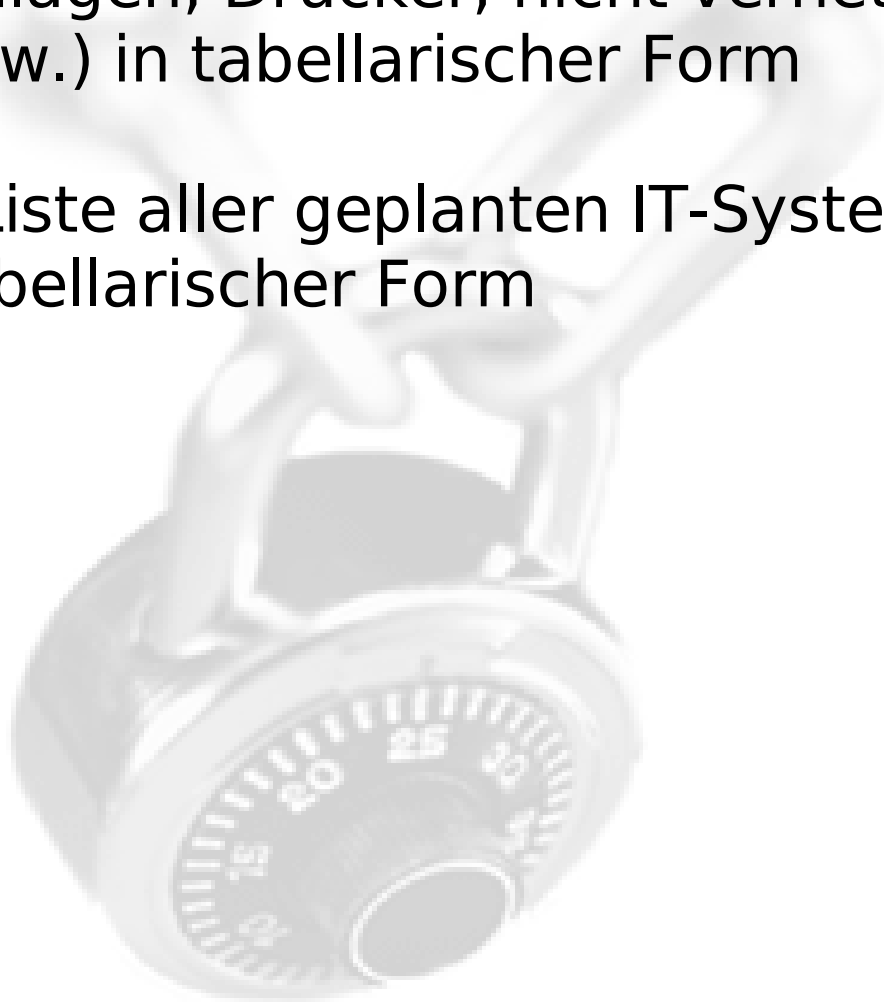
- Erstellung
- Aktualisierung
- Abgleich unter Mitwirkung von Mitarbeitern
- Vorbereitete Checkliste und Management-Programme helfen





## Erhebung der IT-Systeme

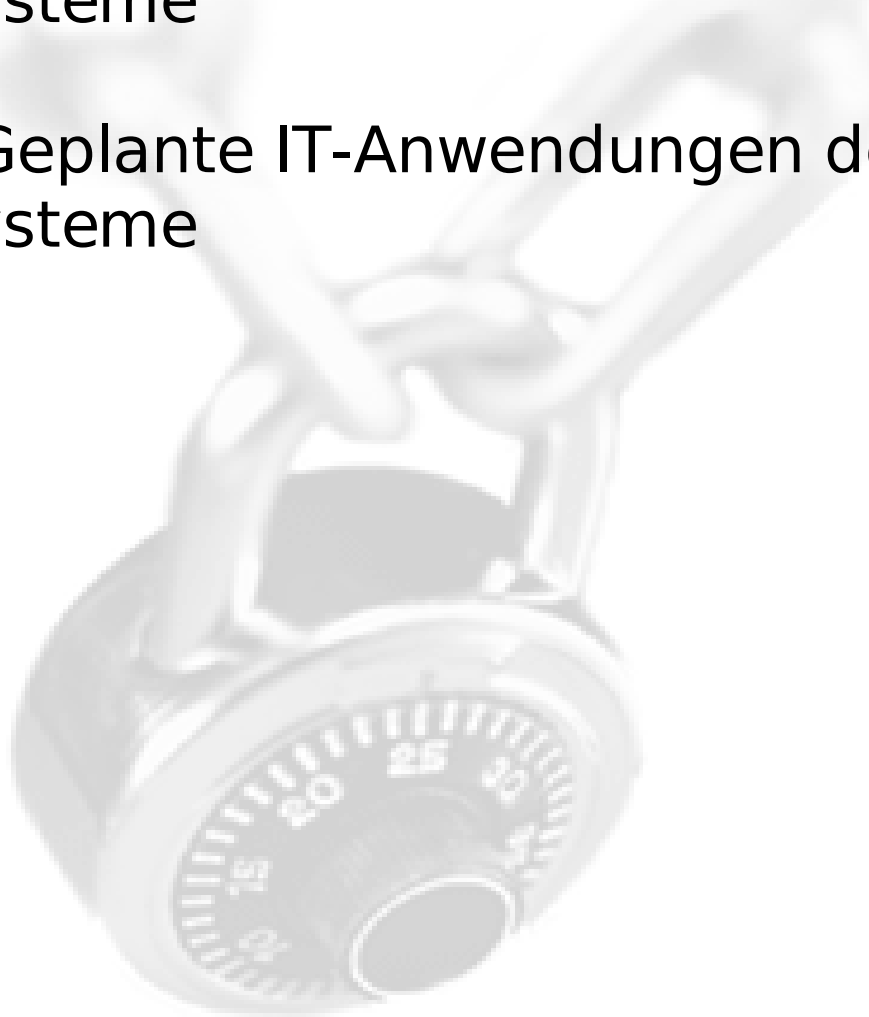
- Liste aller vorhandenen IT-Systeme (auch TK-Anlagen, Drucker, nicht vernetzte Systeme, usw.) in tabellarischer Form
- Liste aller geplanten IT-Systeme in tabellarischer Form

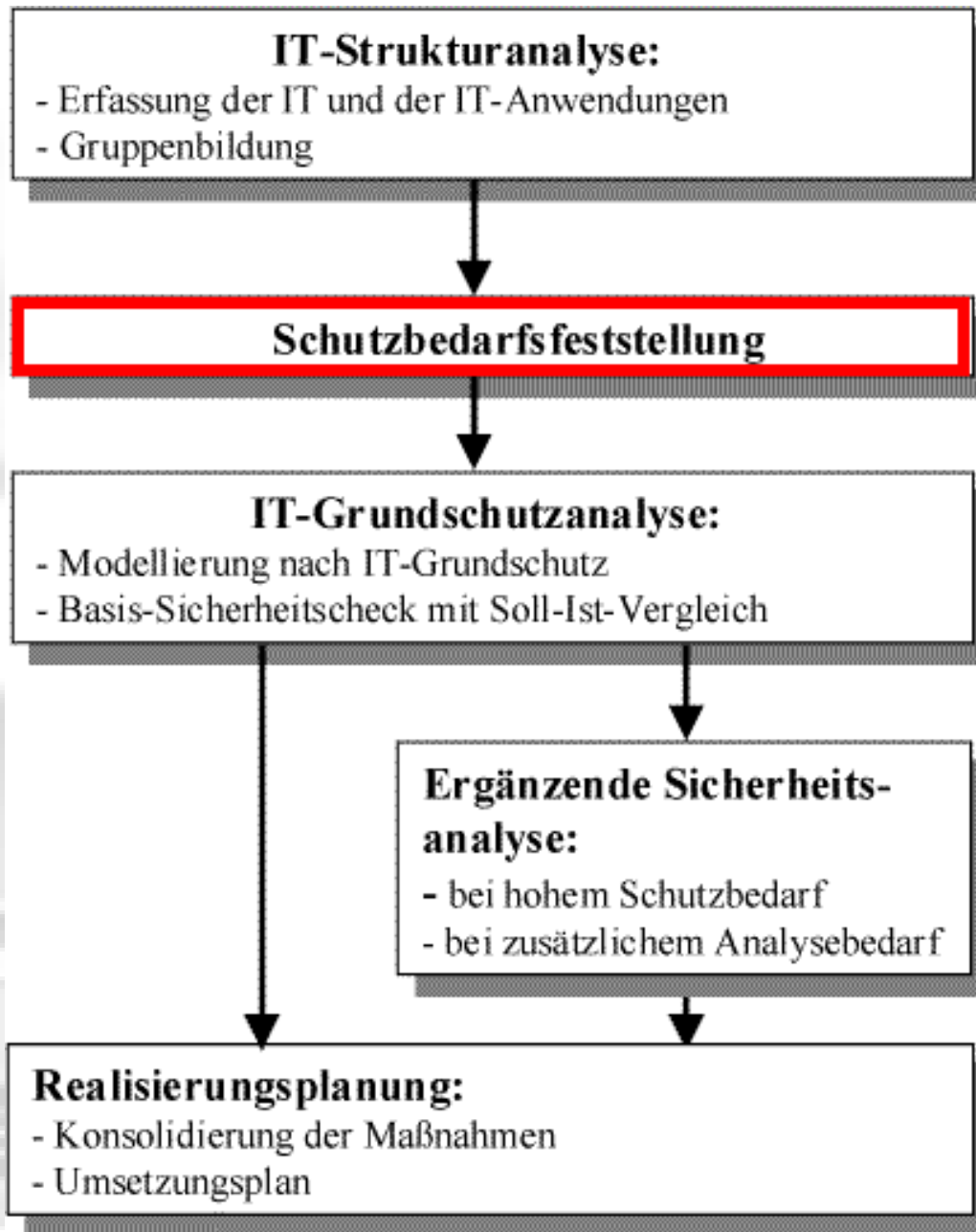




## Erfassung der IT-Anwendungen

- Laufende IT-Anwendungen der wichtigsten IT-Systeme
- Geplante IT-Anwendungen der wichtigsten IT-Systeme







Ziel: Entscheidung, welchen Schutzbedarf jede erfasste IT-Komponente bezüglich

- Vertraulichkeit
- Integrität
- Verfügbarkeit

besitzt.

„Welcher Schaden ist mit einer Beeinträchtigung der betroffenen Systeme verbunden?“

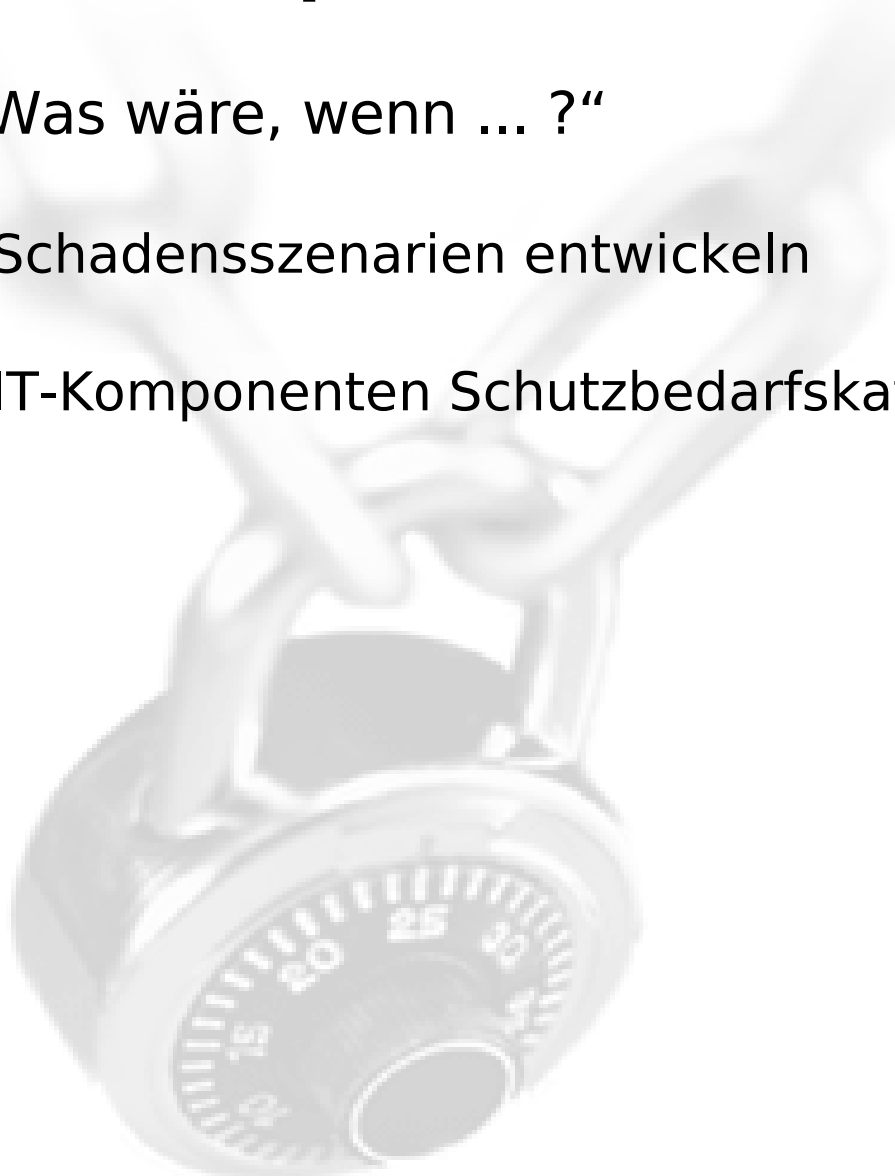




## Workshop mit Mitarbeitern

„Was wäre, wenn ... ?“

- Schadensszenarien entwickeln
- IT-Komponenten Schutzbedarfskategorien zutordnen





## Definition von Kategorien

Schutzbedarf:

- niedrig bis mittel
- hoch
- sehr hoch

Wichtig: Individualisierung der Zuordnungstabelle

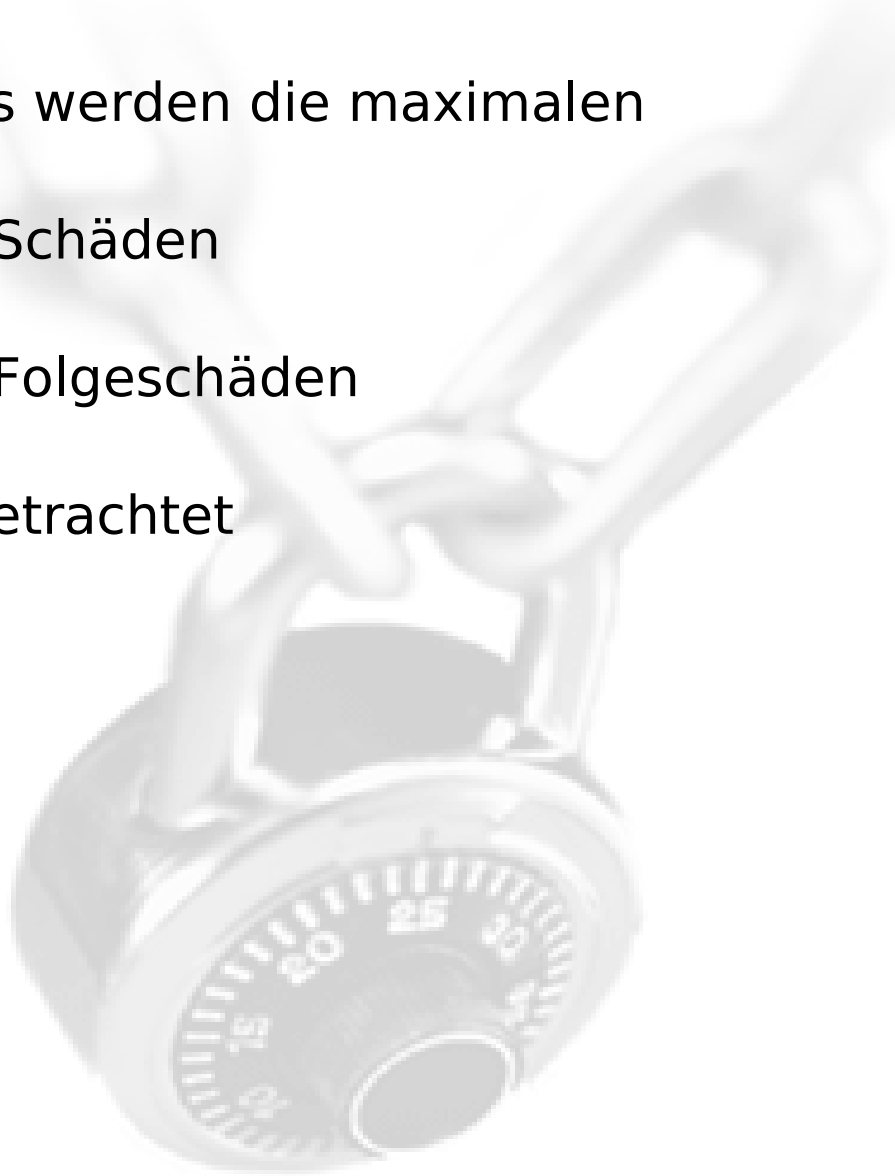


## Betrachtung von Schadensszenarien

Es werden die maximalen

- Schäden
- Folgeschäden

betrachtet





## Dokumentation der Ergebnisse

Als zentrale Dokumentation dient eine Tabelle

### Schutzbedarf wird festgestellt für

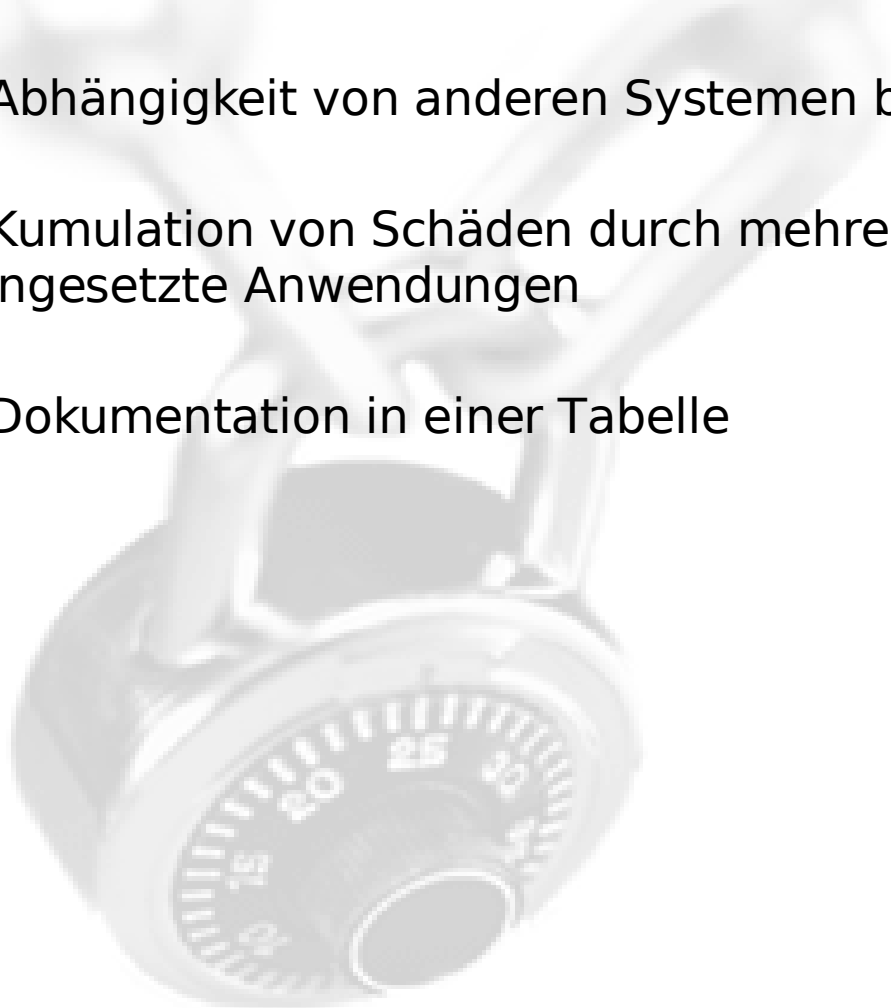
- IT-Systeme
- Kommunikationsverbindungen
- IT-Räume



## Schutzbedarf von IT-Systemen

Schutzbedarf von Systemen hängt direkt ab von den darauf eingesetzten Anwendungen

- Abhängigkeit von anderen Systemen beachten
- Kumulation von Schäden durch mehrere gemeinsam eingesetzte Anwendungen
- Dokumentation in einer Tabelle

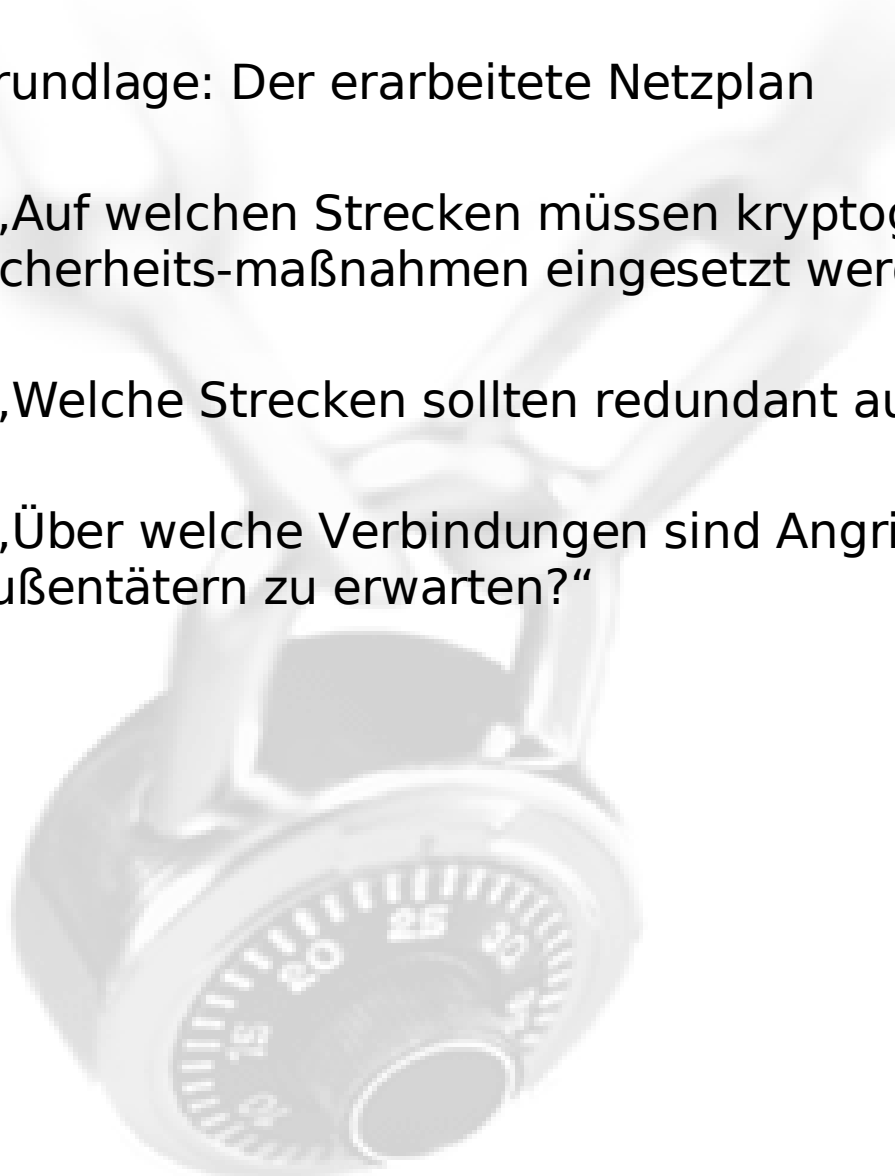




## Schutzbedarf von Kommunikationsverbindungen

Grundlage: Der erarbeitete Netzplan

- „Auf welchen Strecken müssen kryptographische Sicherheitsmaßnahmen eingesetzt werden?“
- „Welche Strecken sollten redundant ausgelegt sein?“
- „Über welche Verbindungen sind Angriffe von Innen- und Außentätern zu erwarten?“

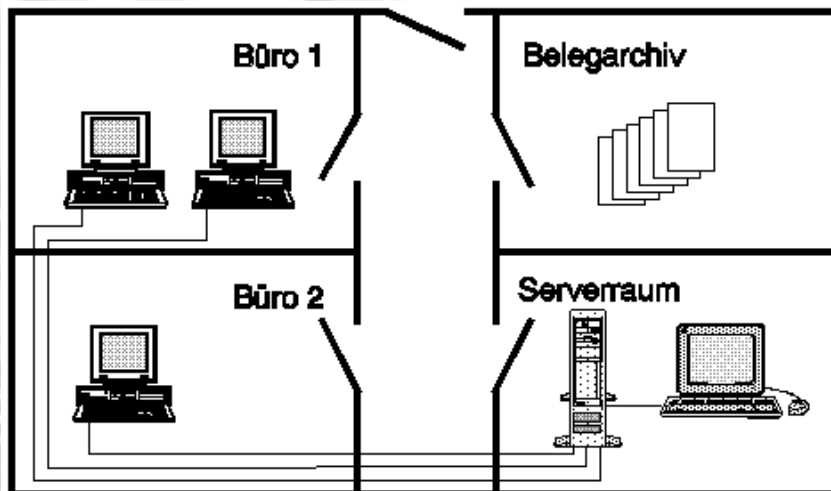




## Schutzbedarf von IT-Räumen

Erstellung einer Übersicht über die Räume, in denen IT-Systeme aufgestellt oder die für den IT-Betrieb genutzt werden. (z.B. Serverräume, Datenträgerarchive, aber auch Büroräume)

- Aus der vorangegangenen Schutzbedarfsfeststellung der IT-Systeme leitet sich der Schutzbedarf von IT-Räumen ab
- Dokumentation in tabellarischer Form

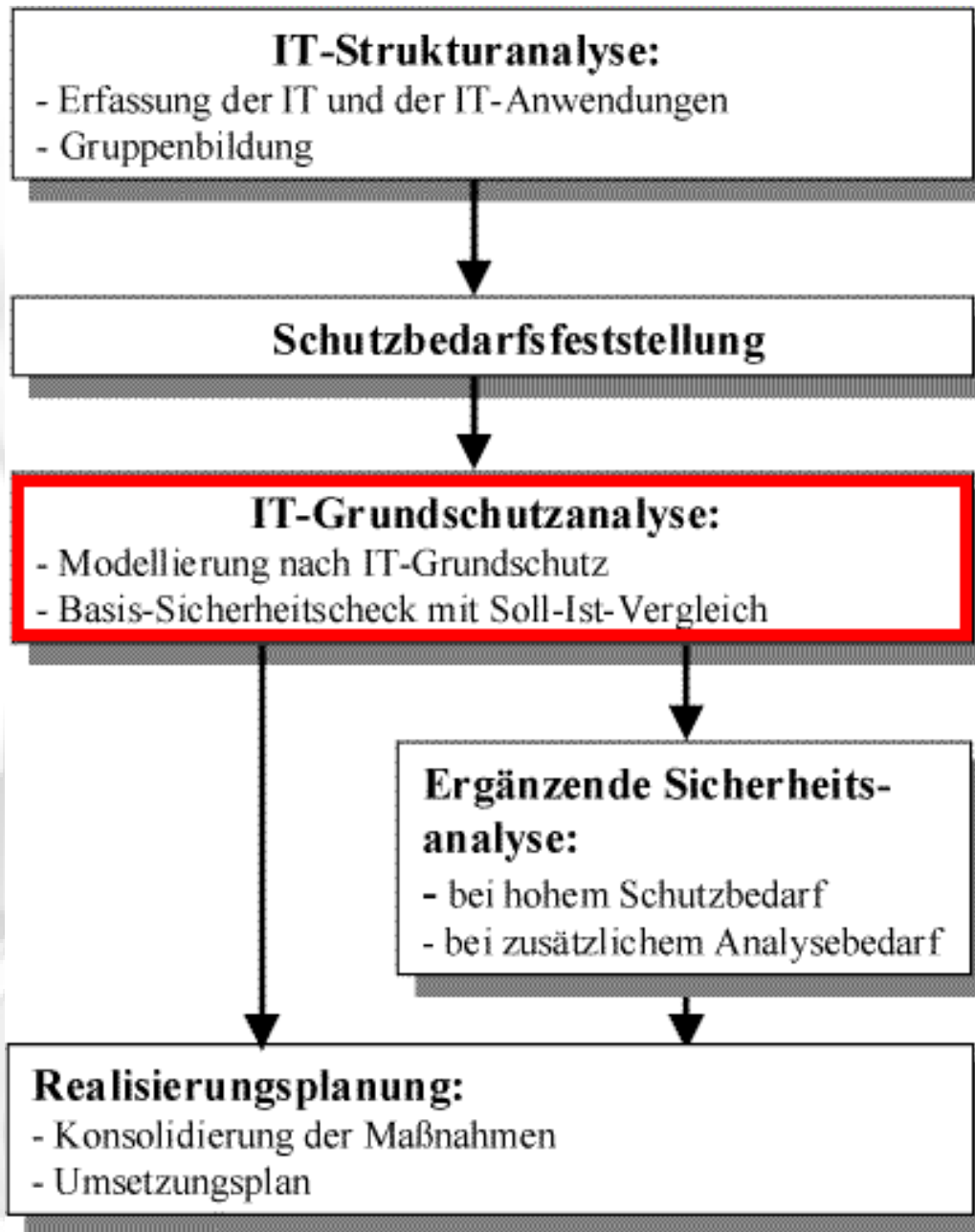




## Interpretation der Ergebnisse

Die Ergebnisse werden ausgewertet und bieten einen Anhaltspunkt für die weitere Vorgehensweise.

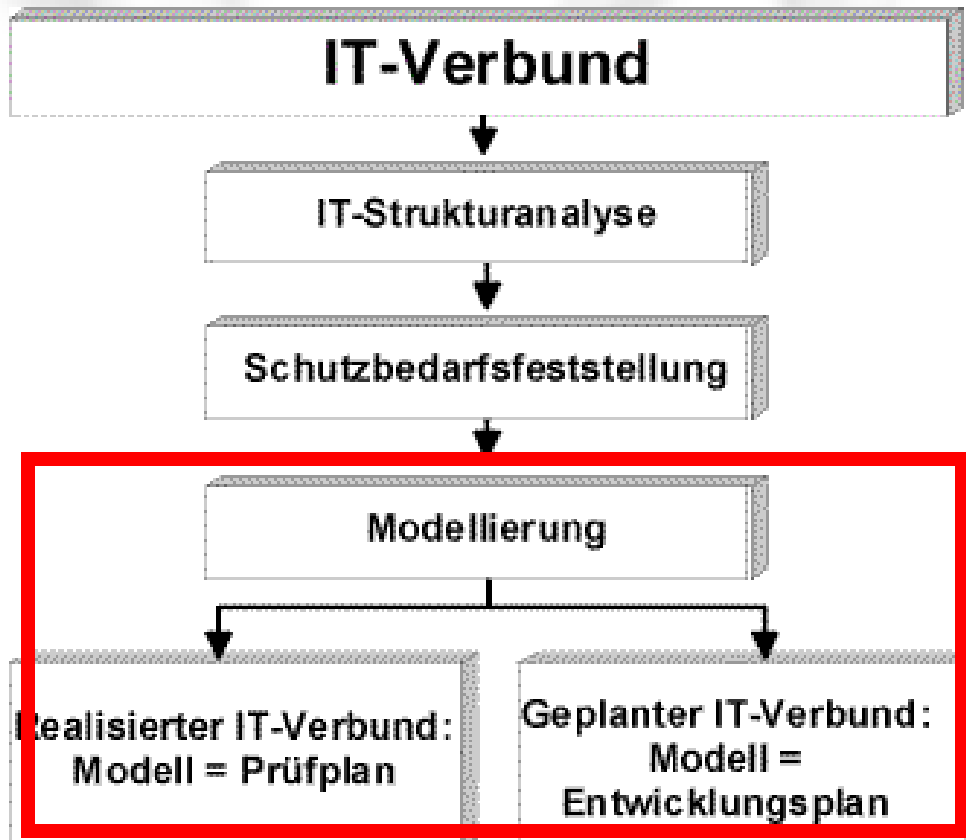


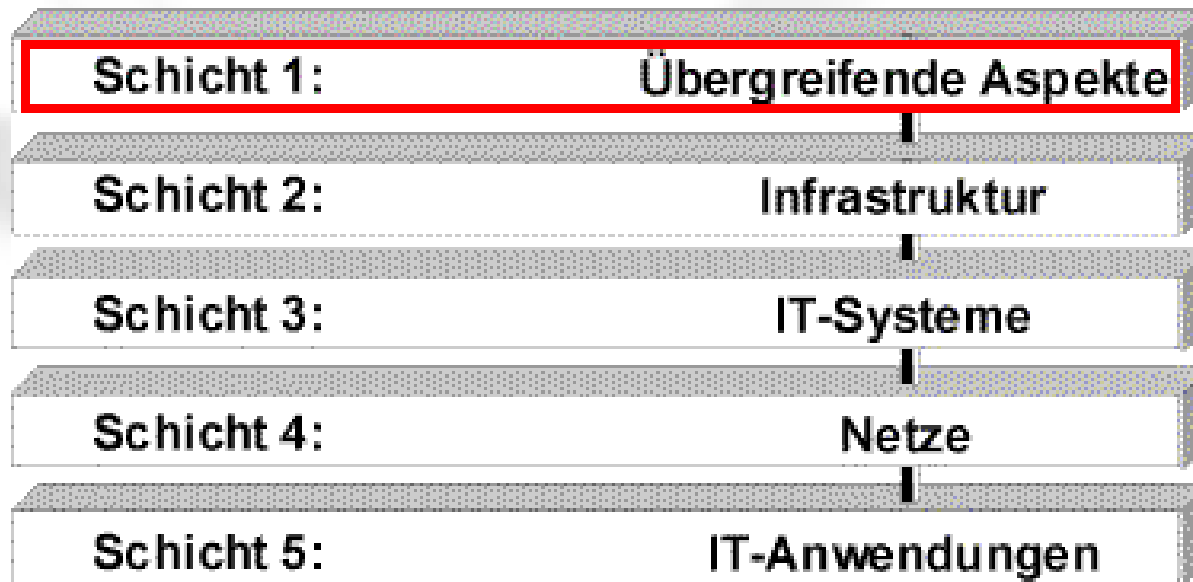




Sicherheitsanalyse auf der Basis des IT-Grundschutzmodells

- Erstellung eines IT-Grundschutzmodells
- Soll-Ist-Vergleich von Sicherheitsmaßnahmen







## Sichtung von

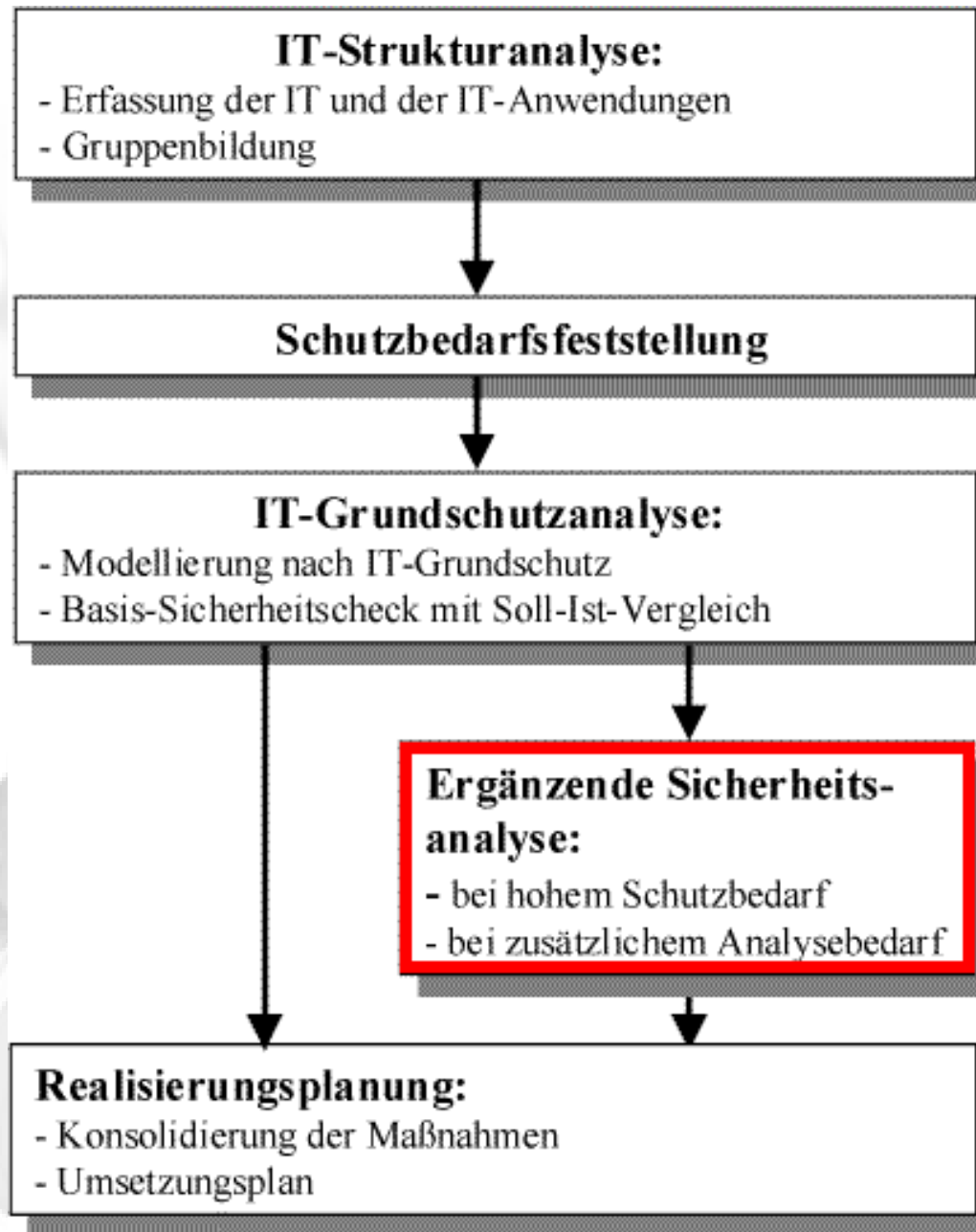
- hausinternen Papieren
  - Verfügungen
  - Arbeitshinweisen
  - Sicherheitsanweisungen
  - „informelle“ Vorgehensweisen,
- welche die sicherheitsrelevanten Abläufe regeln.



Das ermöglicht einen umfassenden Einblick in die organisatorischen Standardmaßnahmen wie

- Datenschutz
- Notfallvorsorge
- Datensicherung
- Virenschutz
- Kryptografie

Stichprobenartige Prüfung von Client- und Servereinstellungen





## Sicherheitsanalyse bei festgestelltem

- hohem
- sehr hohem

## Schutzbedarf

- „Können die Standardsicherheitsmaßnahmen durch höherwertige IT-Sicherheitsmaßnahmen ergänzt oder ersetzt werden?“
- Es werden nur die sicherheitskritischen Bereiche analysiert



## Risikoanalyse

- Relevante Bedrohungen aufgrund vorhandener Schwachstellen herausarbeiten
- Eintrittswahrscheinlichkeit schätzen
- Kombination mit Schutzbedarf, um die bestehenden Risiken zu ermitteln
- Für untragbare Risiken: Wahl von ergänzenden IT-Sicherheitsmaßnahmen

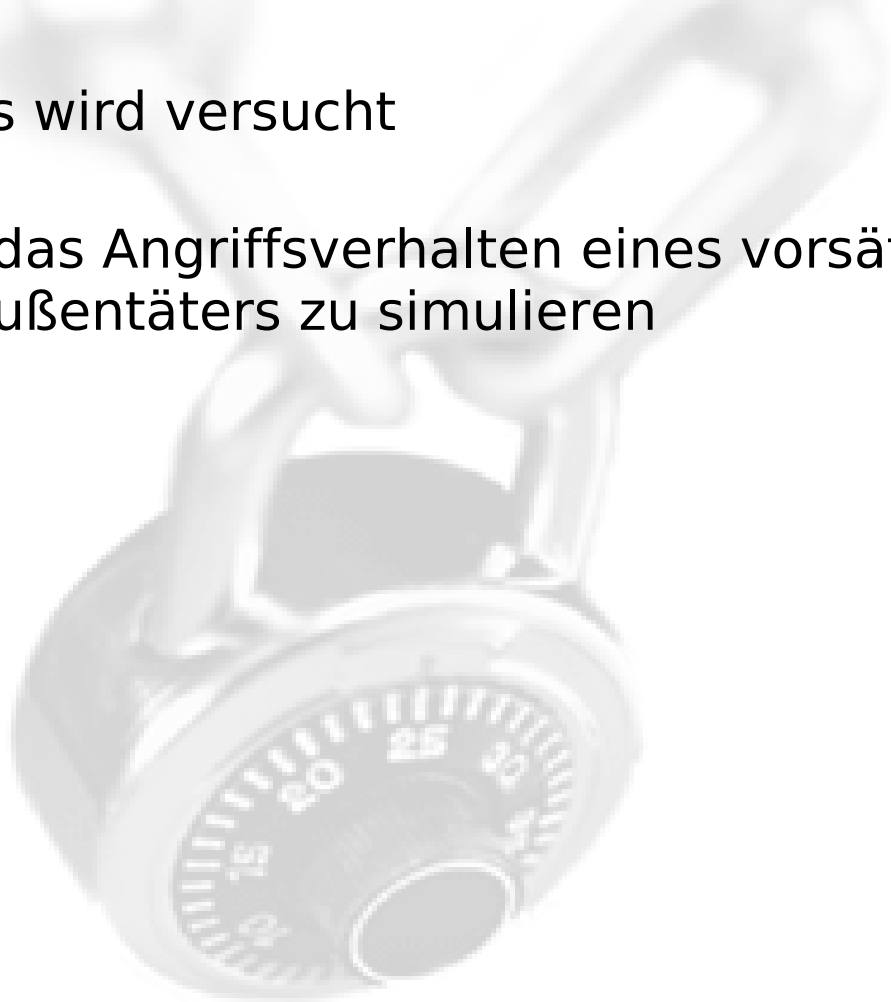


## Penetrationstest

Ziel: Erfolgsaussichten eines vorsätzlichen Angriffs auf den IT-Verbund einschätzen

Es wird versucht

- das Angriffsverhalten eines vorsätzlichen Innen- und Außentäters zu simulieren

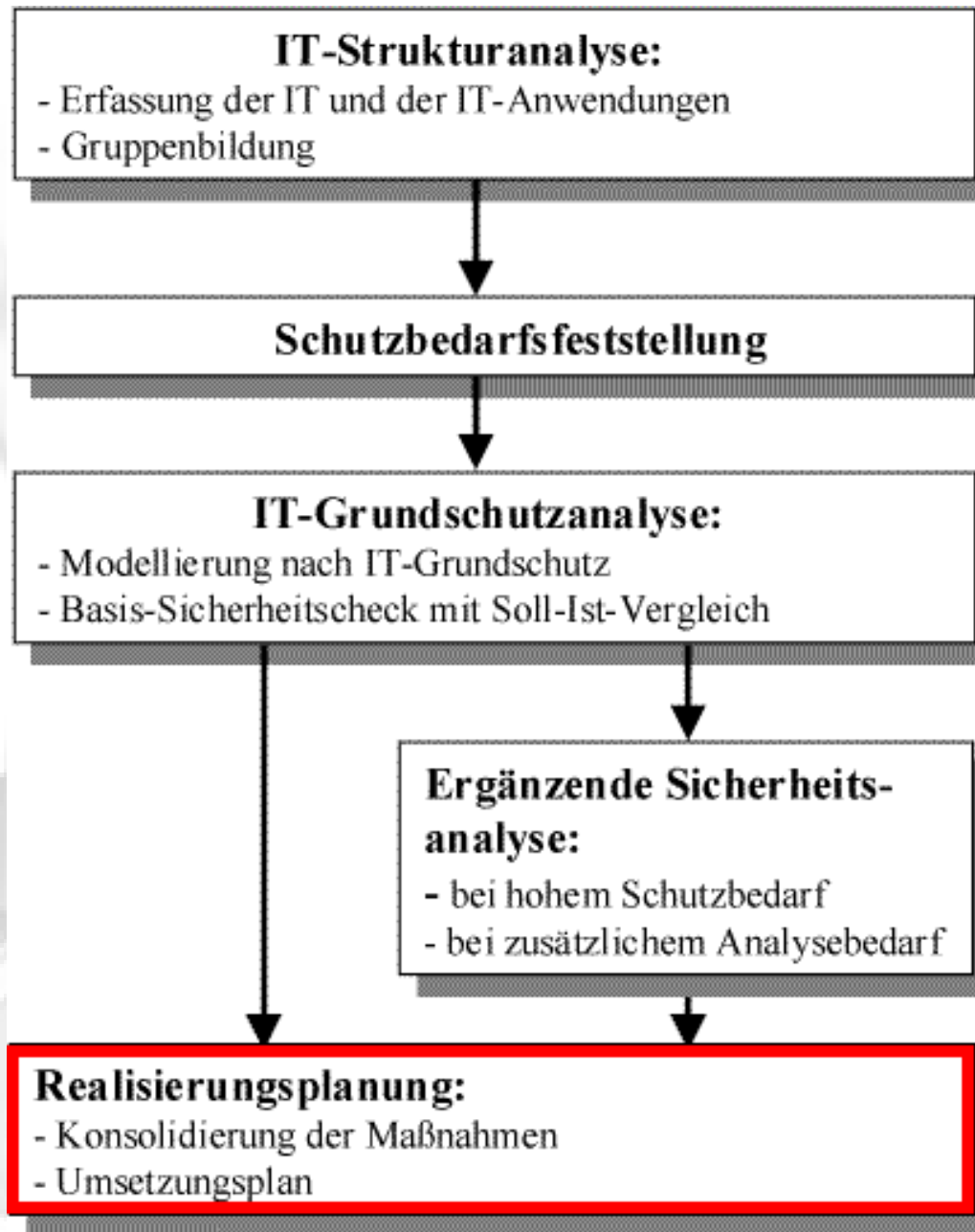




## Differenz- Sicherheitsanalyse

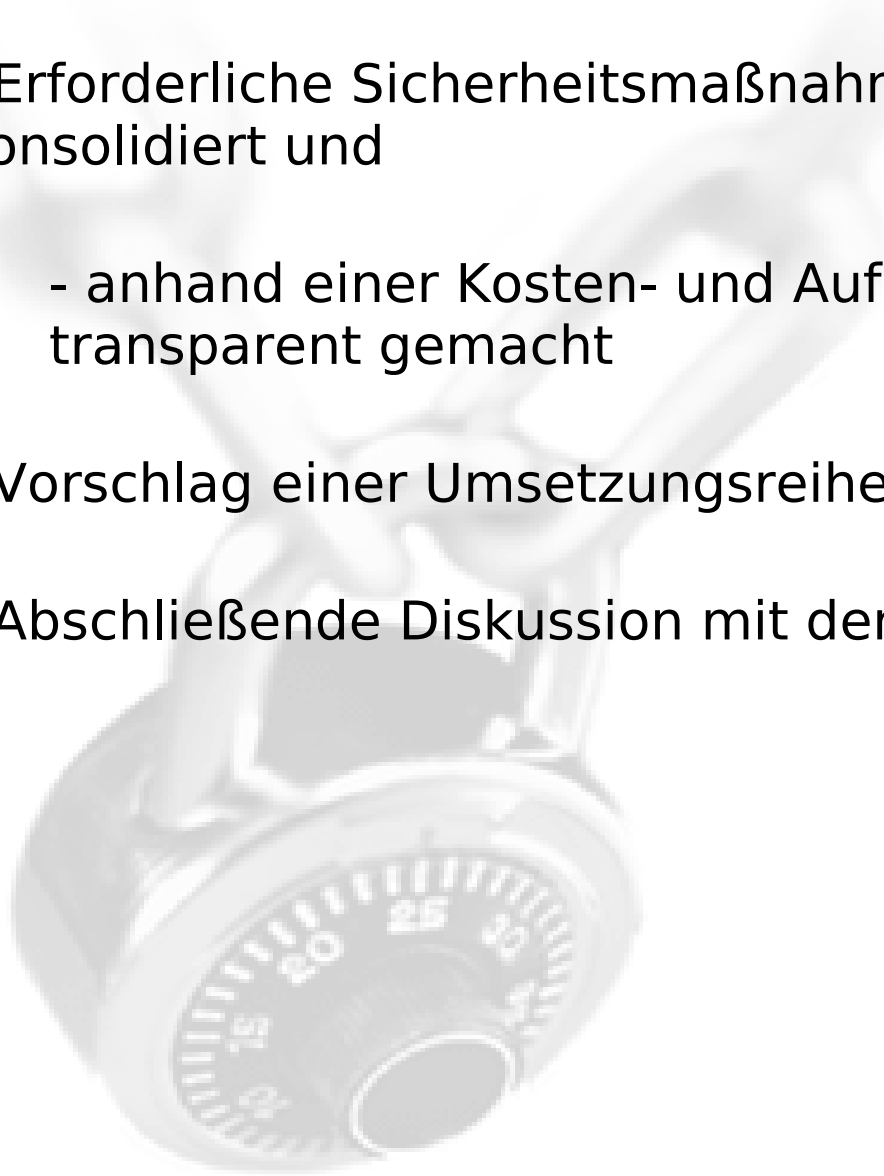
- „Welche IT-Sicherheitsmaßnahmen gehen über die IT-Grundschutzmaßnahmen hinaus?“
- „Welche Schutzmaßnahmen sind optional?“

**Alle Ergebnisse der Sicherheitsanalyse werden tabellarisch erfasst.**





- Sichtung der Untersuchungsergebnisse
- Erforderliche Sicherheitsmaßnahmen werden konsolidiert und
  - anhand einer Kosten- und Aufwandsschätzung transparent gemacht
- Vorschlag einer Umsetzungsreihenfolge
- Abschließende Diskussion mit den Verantwortlichen





# mit Sicherheit – Institut für Business Consulting

Marc McGuinness  
[mcguinness@business-consulting.de](mailto:mcguinness@business-consulting.de)

Download dieser Präsentation unter  
<http://www.psychology4u.de/mcguinness/projects.php3>