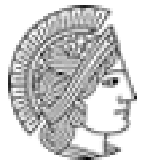


Vorlesung VPN
Fachbereich Informatik
Lehrstuhl Prof. Buchmann

SS-02

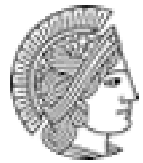
In Zusammenarbeit mit dem CAST-Forum

Dr. Wolfgang Böhmer

Skript: http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/

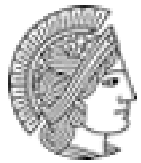
E-Mail: wboehmer@cdc.informatik.tu-darmstadt.de

Vorlesungsinhalte (1/9)



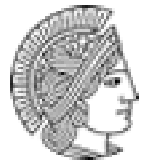
- Einführung / Themenüberblick
  - Was ist ein VPN /Arten / Varianten
- Netzgrundlagen der VPN-Technologie
  - Verfahren der Kommunikationstechnik
  - Offene Kommunikation in Datennetzen
    - OSI-Architekturmodell
    - OSI-Funktionen /Dienste / Protokolle
  - Internet-Protokoll Version IPv4 und IPv6
    - BOOTP/DHCP und Mobile-IP
    - Ende-zu-Ende-Flußkontrolle mittels TCP
    - Dienstgüten (Cos) und (QoS) in IP-Netzen
    - Integrierte Dienste und differenzierte Dienste
    - Multi-Protocol Label Switching (MPLS)

Vorlesungsinhalte (2/9)



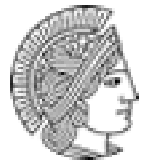
- Weitverkehrsnetze (WAN)
  - Fast-Packet-Switching (FPS)
  - Frame-Relay
  - MPLS über Frame-Relay
  - Asynchroner Transfer Modus (ATM)
  - ATM-Referenzmodell
  - MPLS über ATM-Verbindungen
  - IP/MPLS und Multiprotokoll Lambda Switching (MPλS)

Vorlesungsinhalte (3/9)



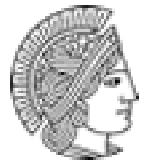
- Informations- und Kommunikationssicherheit
  - Definition IuK-Sicherheit
  - Verfahren zur Erlangung der IuK-Sicherheit
    - Risikoanalysen
    - ITSEC und Common Criteria (CC)
    - Sicherheitsarchitektur offener Systeme
    - Evaluierung der Gesamtunternehmenssicherheit
- Verschlüsselung
  - Verschlüsselungstechniken
    - Substitution und Transformation
  - Symmetrische Kryptosysteme
    - Blockchiffre und Stromchiffre
    - DES, Triple DES, IDEA und AES

Vorlesungsinhalte (4/9)



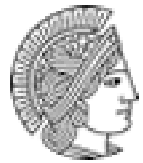
- Asymmetrische Kryptosysteme
- Schlüsselaustauschverfahren
  - Diffi-Hellmann, RSA, ELGamal, DAS
- Digitale Signatur
  - Mechanismen einer digitalen Signatur
- PKI und Trust Center
  - x.500 und x.509v.3
  - Zertifizierung und Validierung
  - PKI-Unterscheidungsmerkmale
  - Einsatz von Digitalen Zertifikaten

Vorlesungsinhalte (5/9)



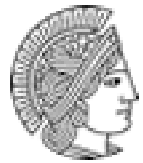
- Verfahren zur Authentifizierung
  - Einfache Authentifizierung
  - Starke Authentifizierung
    - Ein-Wege/ Zwei-Wege/Drei-Wege-Authentifizierung
  - Zwei Faktoren-Authentifizierung in der Praxis
    - Zeitsynchrone mittels Token-Cards
    - Speicherkarten und Smarts-Cards
  - Authentifizierungsverfahren in der Anwendung
    - PPP-Verbindung als Voraussetzung für PAP und CHAP
    - AAA-Sicherhitsarchitektur
    - Radius und TACAS+
    - Kerberos

Vorlesungsinhalte (6/9)



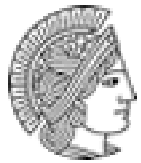
- Varianz der VPN-Typen
  - Intranet-VPN (Site-toSite)
  - Extranet-VPN (End-to-End)
  - Remote-Access-VPN (End-to-Site)
  - Eckpunkte für den Einsatz eines VPN
    - VPN-Sicherheitspolitik
    - VPN und Firewall
    - VPN und Router
    - Quality-of-Service in VPN / DiffServ in VPN
- VPN-Basistechnologien
  - Tunneling
  - Layer-2-Techniken (L2F, PPTP, L2TP, L2Sec)
  - Layer-3-Techniken

Vorlesungsinhalte (7/9)



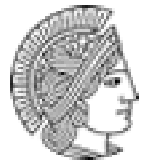
- Sicherheitsstandard für das Internet (IPSec)
  - Das Ziel von IPSec
  - IPSec-Sicherheitsvereinbarungen (SA) / Initiierung und Kombination
  - IPSec-AH-Header
  - IPSec-ESP-Header
  - IPSec und Remote Access
  - Internet-Key-Exchange-Management (IKE) (Phase-1 /Phase-2)
  - ISAKMP/Oakley und Skip
  - Layer-2- und Layer-3-Vergleich
- Layer-4-Techniken
  - Secure Socket Layer (SSL) und Transport Layer Sicherheit (TLS)
  - Vergleich IPSec und SSL/TLS
- Layer-5-Techniken
  - Socks V.5

Vorlesungsinhalte (8/9)



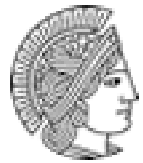
- Provider-Netze - sicherer Kommunikation über fremde Netze
  - Provider-Netze und Netzstrukturen
    - IP-VPN über Wählverbindungen
    - VPN über fremde Netze
    - Referenzmodell für ein CE-basierendes VPN
    - Referenzmodell für ein NB-basierendes VPN
  - Netzwerk-Performance und Management
    - Sicherheitsaspekte
    - Service-Vereinbarungen (SLA)
  - VPN-Klassifizierungen
- Einsatz von Virtual Private Networks
  - VPN-Marktbetrachtungen
  - IPSec und MPLS für VPN der zweiten Generation
    - IPSec und Performance Aspekte

Vorlesungsinhalte (9/9)



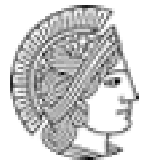
- Planungsaspekte
- Phasenplan zur Durchführung eines VPN-Projektes
  - Analyse
  - Konzept
  - Realisierung
  - Betrieb

Informations- und Kommunikationssicherheit



- Grenzen zwischen traditionellen und modernen Kommunikationsmittel lösen sich mehr und mehr auf
- Grundsätzlich zwei verschiedene Typen von Kommunikationsnetzen
  - Verteilnetze: Alle Teilnehmer bekommen vom Netz die gleiche Information (Fernsehen, Radio). Jeder Teilnehmer wählt lokal aus was er empfangen will.
  - Vermittlungsnetze: Jede Teilnehmerstation erhält vom Netz individuell nur das was vom Teilnehmer angefordert oder geschickt wurde. Es wird generell in zwei Richtungen kommuniziert.
- Aufbau von neuen Informationssystemen bringt nicht nur Vorteile, Risiken und Gefährdungen müssen ebenso in Betracht gezogen werden.
- Zu Vertiefung dieser Frage werden Schutzziele und Mechanismen betrachtet
  - Duale IT-Sicherheit
    - Verlässlich
    - Beherrschbar

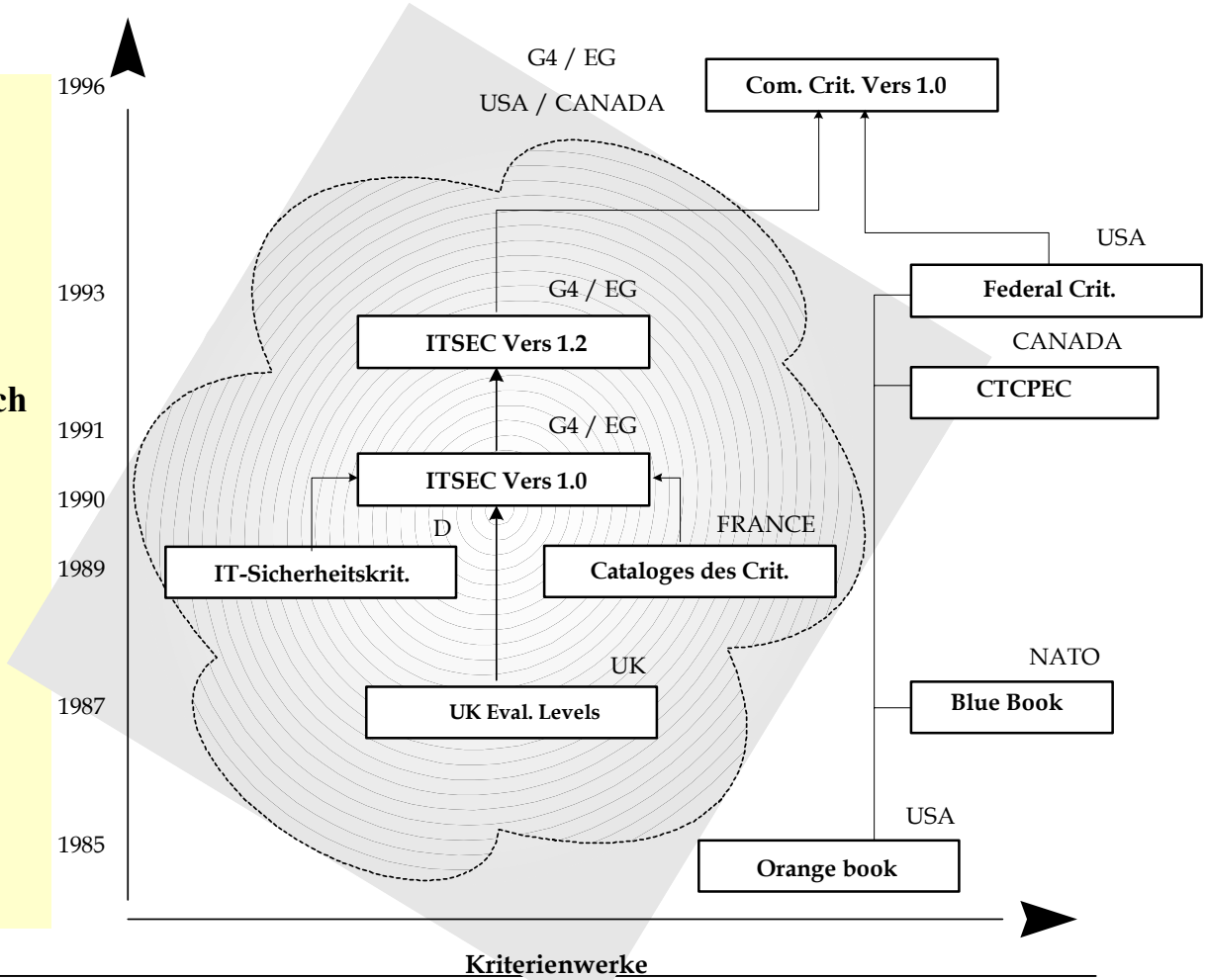
Die fünf Hauptaspekte der IuK-Sicherheit



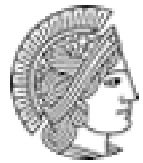
- Definition der IuK-Sicherheit
  - Vertraulichkeit *(confidentiality)*
  - Integrität *(integrity)*
  - Verfügbarkeit *(availability)*
- Ergänzung Benutzersicht
  - Zurechenbarkeit *(accountability)*
  - Verbindlichkeit *(liability)*
- Hauptaspekte der IuK-Sicherheit sind Ziele eines jeden IT-Sicherheitskonzept
  - Unterbrechung, gerichtet gegen die Verfügbarkeit
  - Abhören, gerichtet gegen die Vertraulichkeit
  - Fälschung gerichtet gegen die Authentifizierung
  - Modifikation gerichtet gegen die Integrität

Verfahren zur Erlangung der IuK-Sicherheit

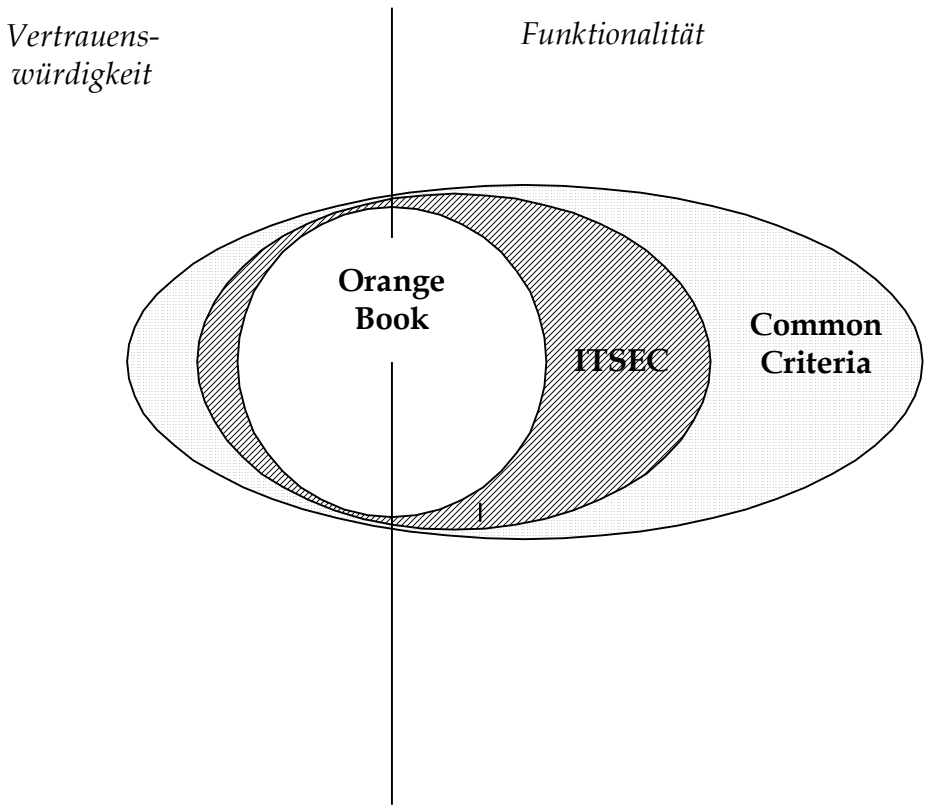
- **IuK-Sicherheit nicht nur technisch orientiert**
- **Beginn von Kriterienwerken ca. 1985 (Orange Book)**
- **Europäisches Modell ITSEC ca. 1990**
- **BSI-IT-Grundschutzhandbuch**
- **(erfreut sich großer Beliebtheit)**
- **BSI-IT-Sicherheitshandbuch**
- **(kaum angenommen)**



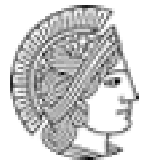
Kriterienwerke im Vergleich



- Viele Gemeinsamkeiten zwischen ITSEC und CC
- Z.B. EAL2 der CC entspricht der Stufe E1 der ITSEC
- ITSEC-Funktionsklassen wird durch die CC-Schutzprofile abgelöst.
- CC deckt das größte Spektrum der Vertrauenswürdigkeit und Funktionalität ab



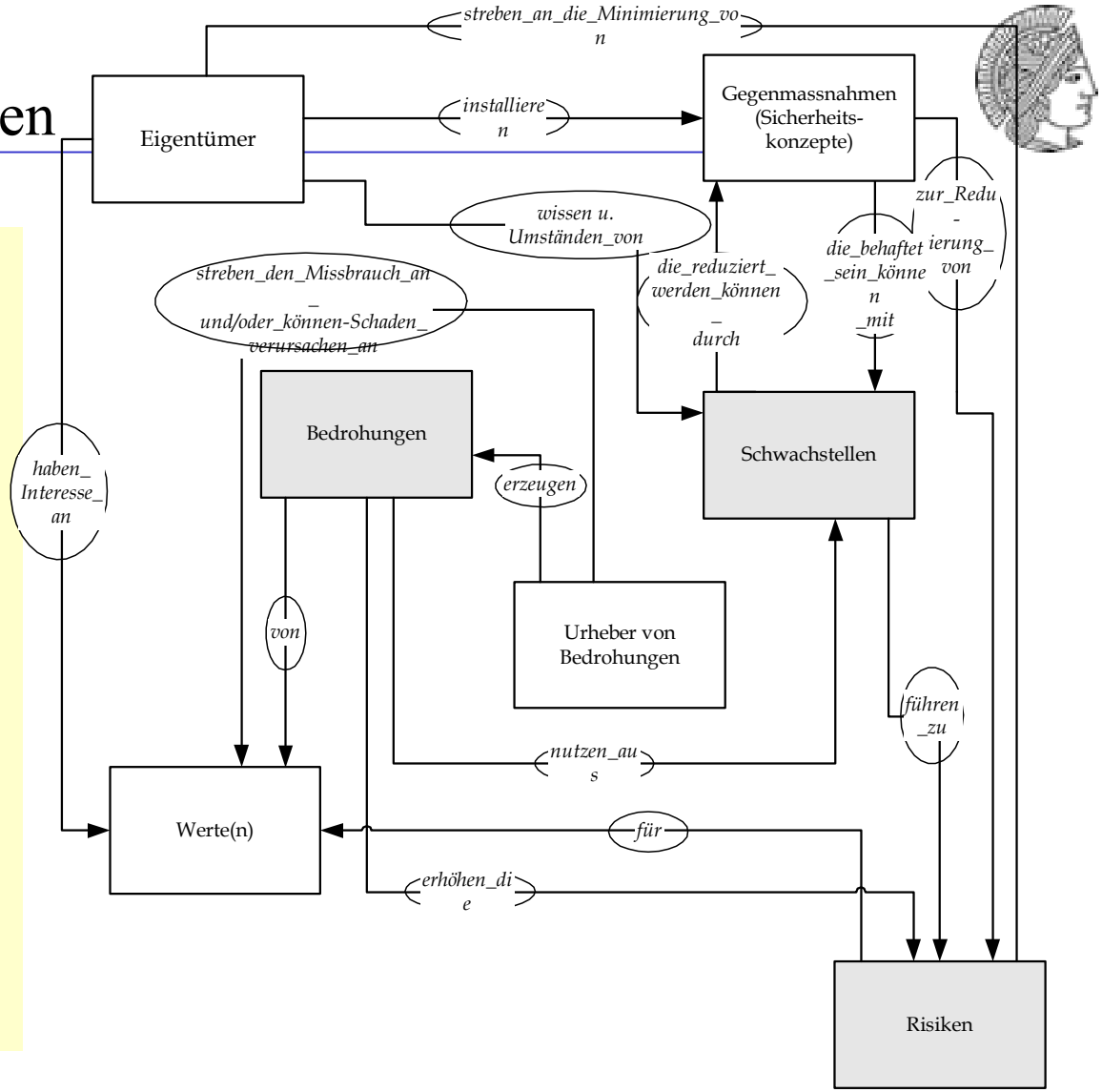
Risikoanalyse *(Schutzbedarf hoch bis sehr hoch)*



- Versicherungsgesellschaften haben schon immer das Risiko kalkuliert
- Risiko-Definition nach DIN, VDE NORM 3100
  - **Risiko: Produkt von möglichen Eintrittsereignissen von auftretenden Schäden**
- Wechselbeziehung zwischen Werten, Schwachstellen, Bedrohungen, Risiken
- Schutz von Werten mittels Sicherheitskonzept fällt in den Verantwortungsbereich der Eigentümer von Werten

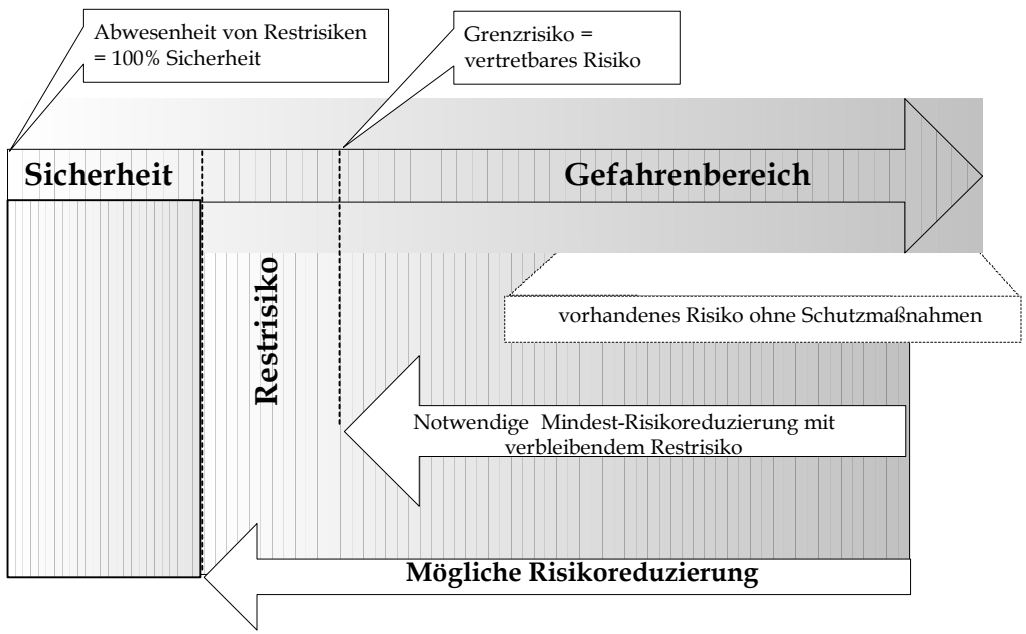
Wechselbeziehungen

- **Bedrohungen und Schwachstellen bilden die Voraussetzung für mögliche Risiken**
- **Was ist Sicherheit?**



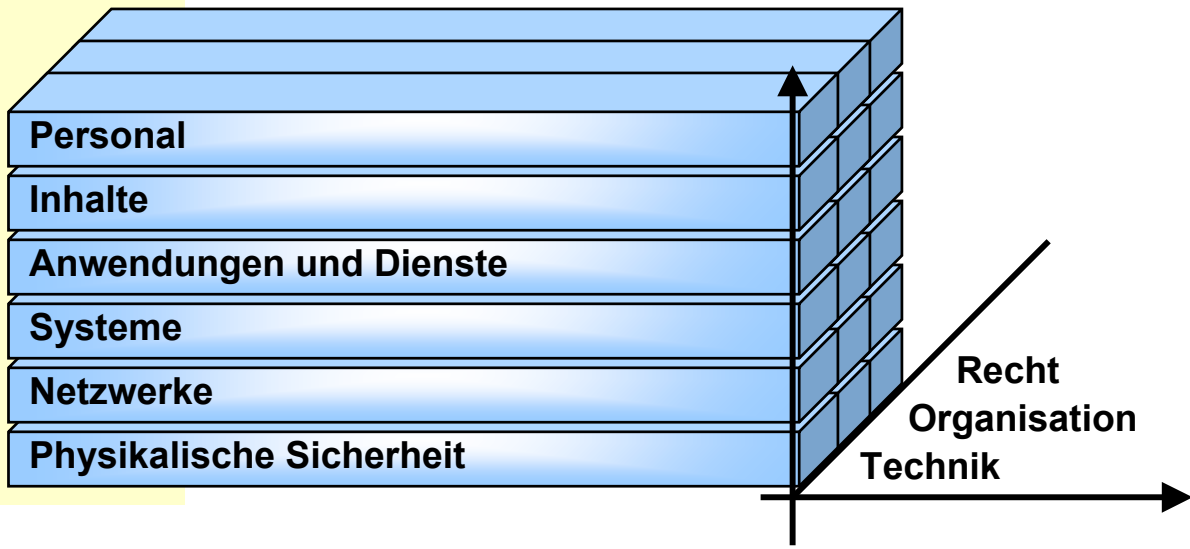
Risikoachse

- **Sicherheit ein relativer Begriff, lässt sich nur durch die Restrisiken näher bestimmen.**
- **100% Sicherheit trifft zu, wenn keine Restrisiken mehr existieren**
- **Minimierung von Restrisiken ist das Ziel von Sicherheits-konzepten und deren Umsetzungen**



Architekturmodell

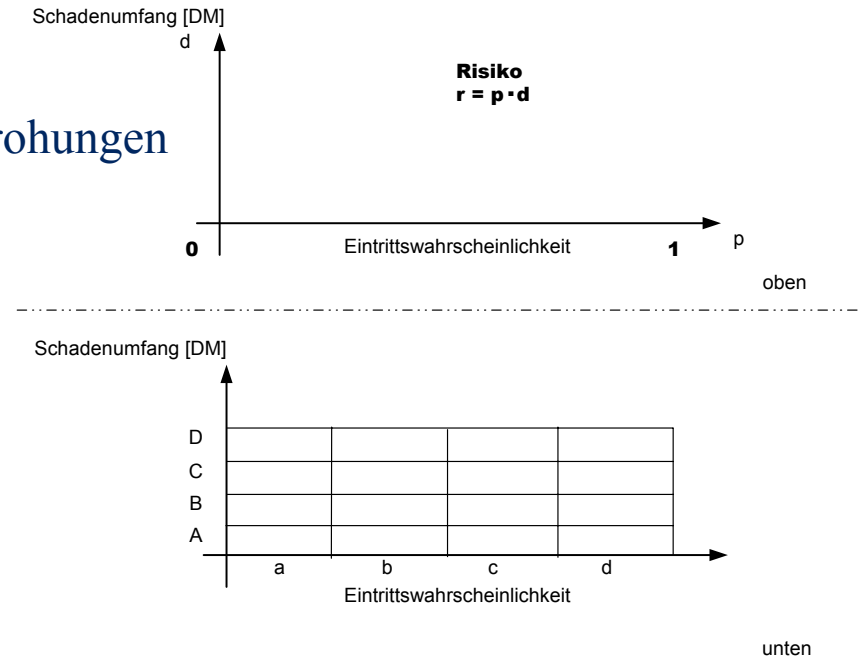
- Reduktion der Komplexität durch ein Architekturmodell
- Jede horizontale Ebene wird mit jeder vertikalen Ebene verknüpft
- Statische und dynamische Prüfung



Risikobestimmung mittels Szenarien

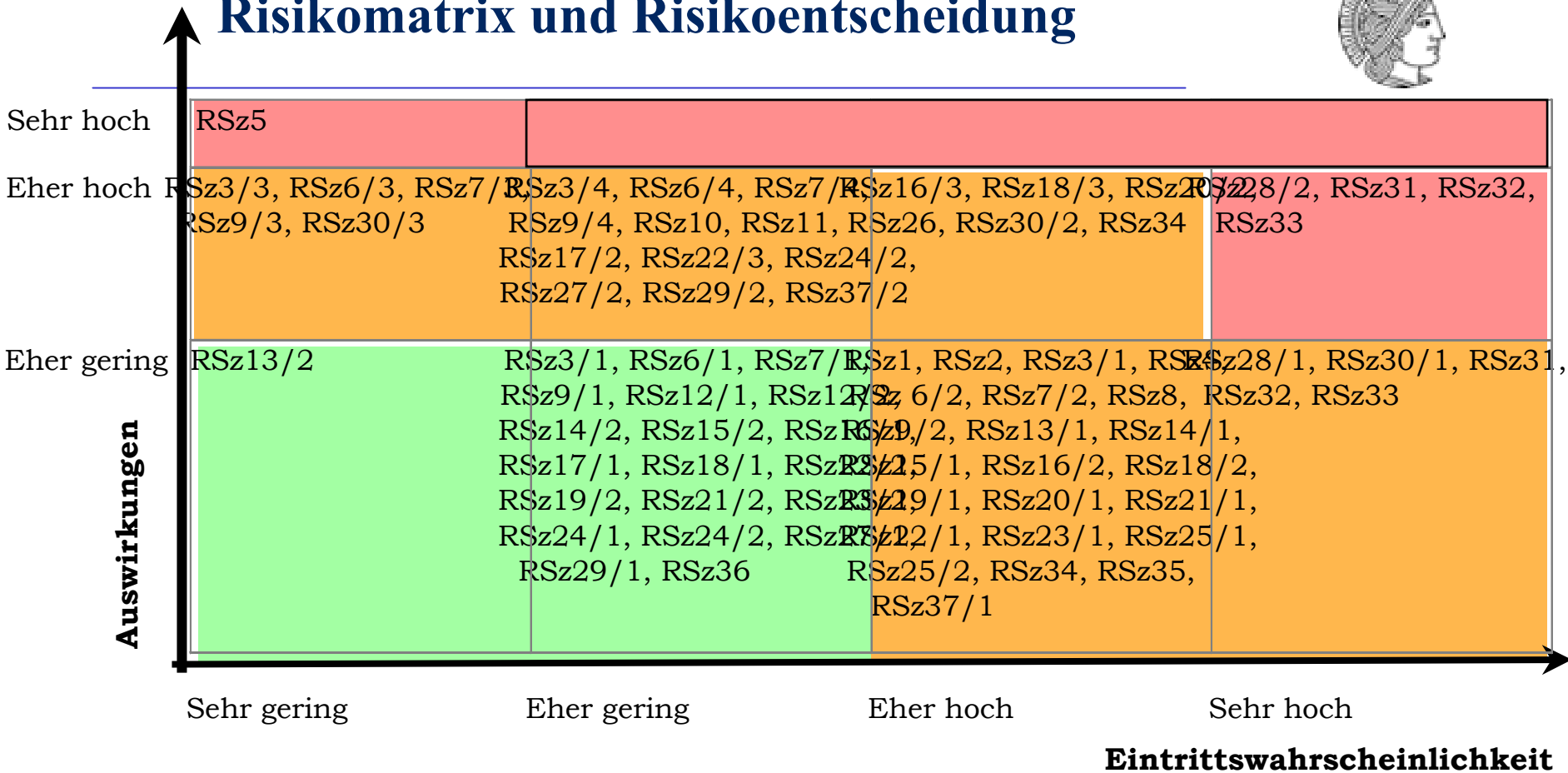
- Grundlage: Daten der IST-Aufnahme
- Diskussion der Schwachstellen und Bedrohungen
- Risikobetrachtung und Szenarienbildung

Risikoformel
nach DIN 3100:

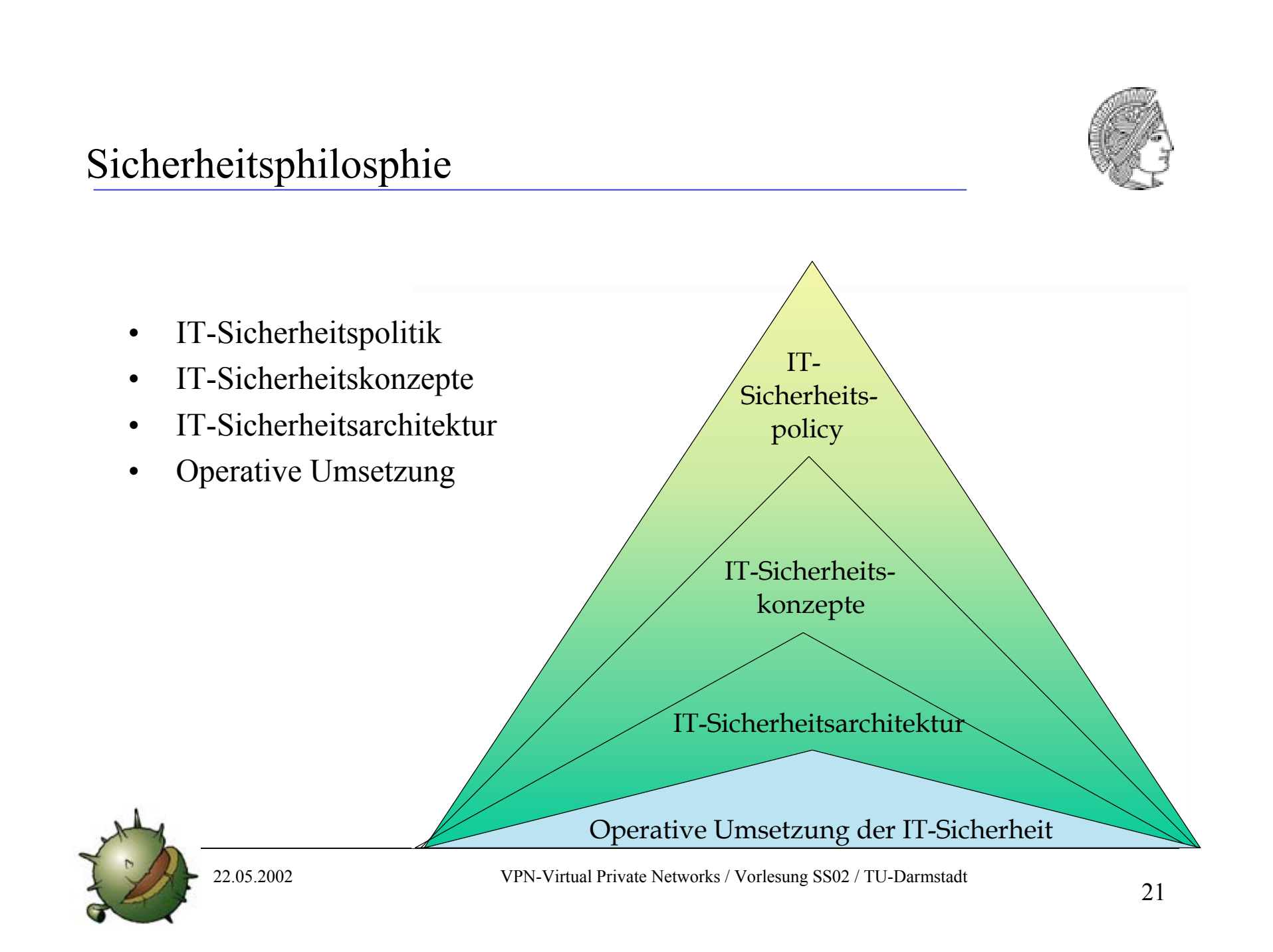


$$R = Ep * Scha \Rightarrow \sum_{i=1}^{n} Rsz_i = Ep_{\left(\sum_{j=1}^{l} b_j \bullet \sum_{k=1}^{m} Schw_k\right)} \bullet Scha$$

Risikomatrix und Risikoentscheidung



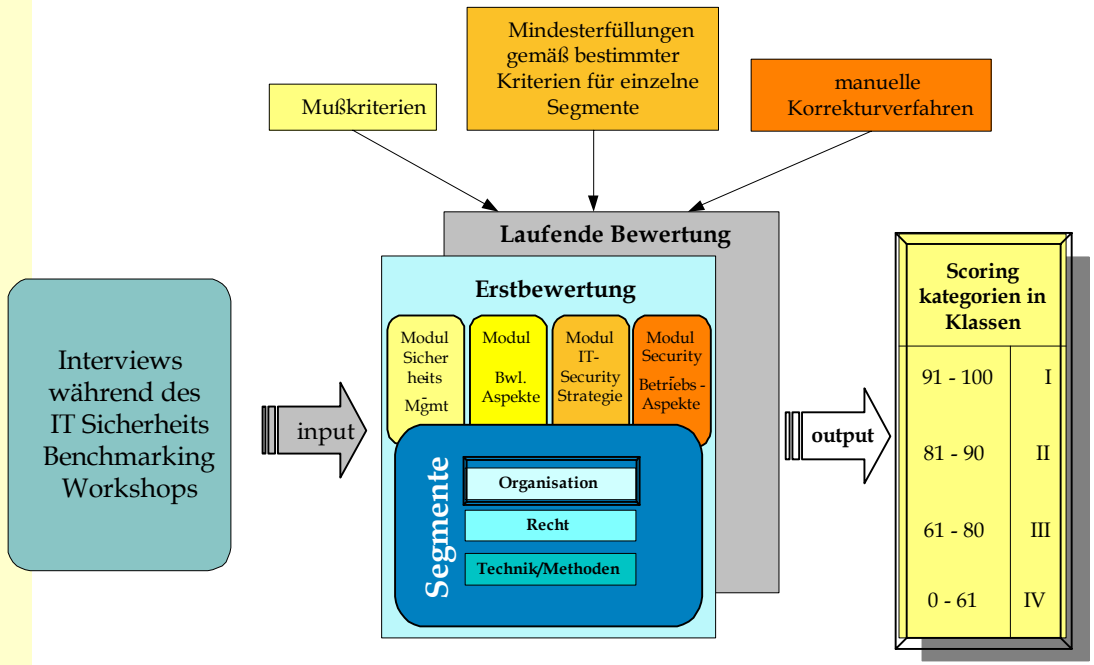
Sicherheitsphilosphie



- IT-Sicherheitspolitik
- IT-Sicherheitskonzepte
- IT-Sicherheitsarchitektur
- Operative Umsetzung

Evaluierung der Unternehmenssicherheit

- Diagnostisches Verfahren
  - Metrische Kennzahlen und
  - Empirisch Kennzahlen
- Entlehnt von der Lieferanten-bewertungsmethode
- Aufuteilung in Segmente / Module / Hauptkriterien
  - Sicherheitsmanagement
  - Betriebswirtschaft
  - IT-Security Strategie
  - IT-Security Betrieb



Evaluierung der Hauptkriterien

- Gewichtung der Hauptkriterien ist vorgegeben
- Struktur ist ähnlich wie ein Verzweigungs-baum

Beispiel Modul: ***Sicherheitsmanagement***

Gewicht	Segment	Hauptkriterium	Nebenkriterium	Gewichtung	Punkte (0-4)	Indexergebnis Beispiel Kunde A
40 %	Organisation	*Personen / Kompetenzen* 30%	Verantwortlichkeit	17,9%		
			Leitung	17,9%		
			Befugnisse	17,9%		
			Datenschutz	10,6%		
			IT-Sec.-Administration	10,7%		
			IT-Revision	14,3%		
			Notfallmanagement	10,7%		
		Dokumente / Konzepte 30%	IT-Sicherhgeitspolitik	21,7%		
			IT-Sicherheitskonzepte	21,7%		
			Schutzbedarf /Kategorie	21,7%		
			Dokumentenklassifizier.	21,7%		
			Notfallpläne	13,2%		
		Formale Kriterien 10%	Bezug zum BS-7799	26,7%		
			Bezug zu CoBit	26,7%		
			Bezug zum GsHB	20,7%		
			Bezug zum ISO-17799	26,7%		
		Sicherheitsprozeß 30%	Definition/Initiierung	18,5%		
			Erstellung v. Richtlinien	18,5%		
			Umsetzung d. Vorgaben	18,5%		
			Auditierung	18,5%		
			Sanktionen	14,8%		
			Fortschreibung	11,1%		
25 %	Recht					
35%	Technik/ Methoden					

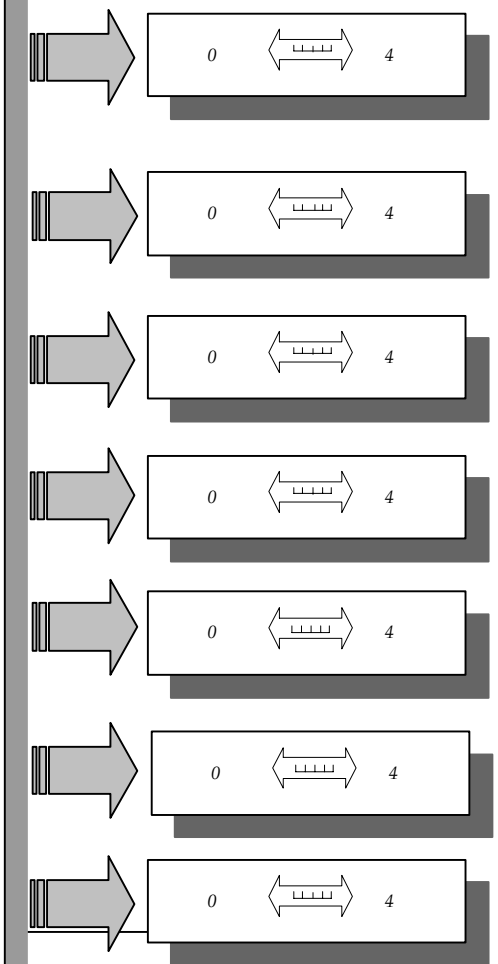
Nebenkriterium

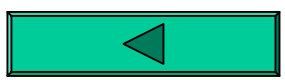
Modul: ***Sicherheitsmanagement*** **- Segment:** ***Organisation*** **- Hauptkriterium:** ***Personen/ Kompetenzen*** **- Nebenkriterien: siehe unten**

- **Nebenkriterien am Beispiel Personen /Kompetenzen bezogen auf eine 5 Pkt. Werteskala**

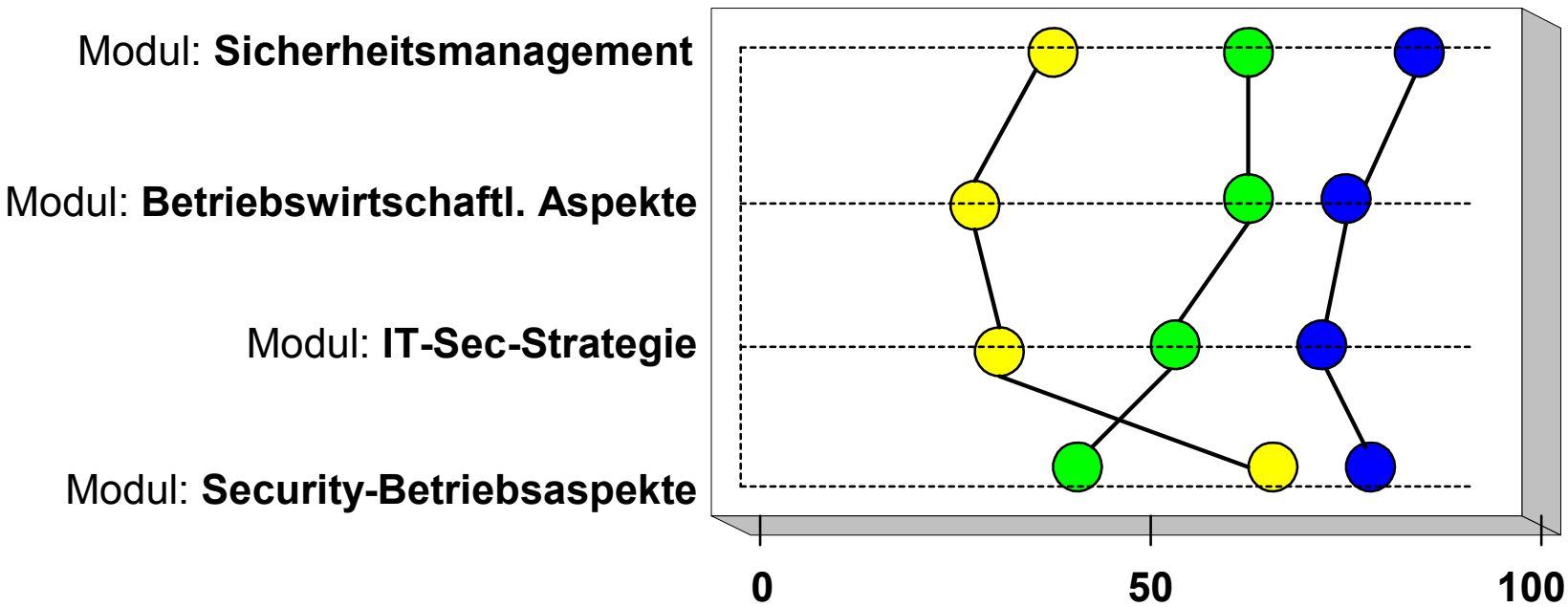
Personen / Kompetenzen

- Verantwortlichkeit
  - keine vorhanden
  - einzelne Admins im Vantwortungsbereich
  - einzelne Sicherheitsvantwortliche koordinieren
  - zentraler Sicherheitsbauftr koor.diniert
  - Ausgeprägte hierarische Strukturen vorhanden
- Leitung
  - Aufgabe wird nicht wahr genom.men
  - Aufgaben nimmt CISO wahr
  - Aufgabe nimmt Vorstand wahr
  - Aufgabe nimmt GF wahr
- Befugnisse
  - Keine Befugnisse
  - Nur empfehlender Charakter der Befugnis
  - Nur auf Abteilungsebene
  - Nur für die IT-Abtl.
  - Unternehemnsweite Befugnis
- Datenschutz
  - existiert ein aktiver Datenschutz
  - Ist der Datenschutzbeauftragte ins IT-Sicherheitsmanagement eingebunden?
- IT-Revision
  - Existiert Fachpersonal für die IT-Revision?
  - Wird IT-Revision mit der reg. Revision abgedeckt?
  -
- Notfallmanagement
  - Es ist kein Notfallmanagement vorhanden
  - Es sind einzelne isolierte Notfall-Verantw. vorhan..
  - verschiedene N-Verantwortliche arbeiten zusam.
  - Ein zentraler N-Verantwortlicher koordiniert
  - Ein komplettes Notfall-Magement ist vorhanden.
- IT-Sec-Administration
  - Existieren spezielle Sicherheits-Admins?
  - Nur für bestimmte Bereiche , bzw. Betriebssysteme
  - Es existieren unternehmensweit IT-Sec-Admins?



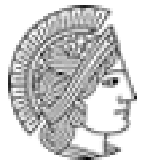


Scoring-Ergebnisse



- Branchendurchschnitt
- betrachtetes Unternehmen
- Best-inClass

Literatur



- **http://www.tu-darmstadt.de/vvss02/comments/20.183.tud**
- **Huston G.: Internet Performance Survival Guide, QoS Strategies for Multiservice Networks, ISBN 0-471-37808-9**
- **Comer, 1995: Internetworking with TCP/IP Vol. I., ISBN 0-13-216987-8**