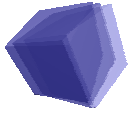




# Einführung in das Nachmittagsprogramm

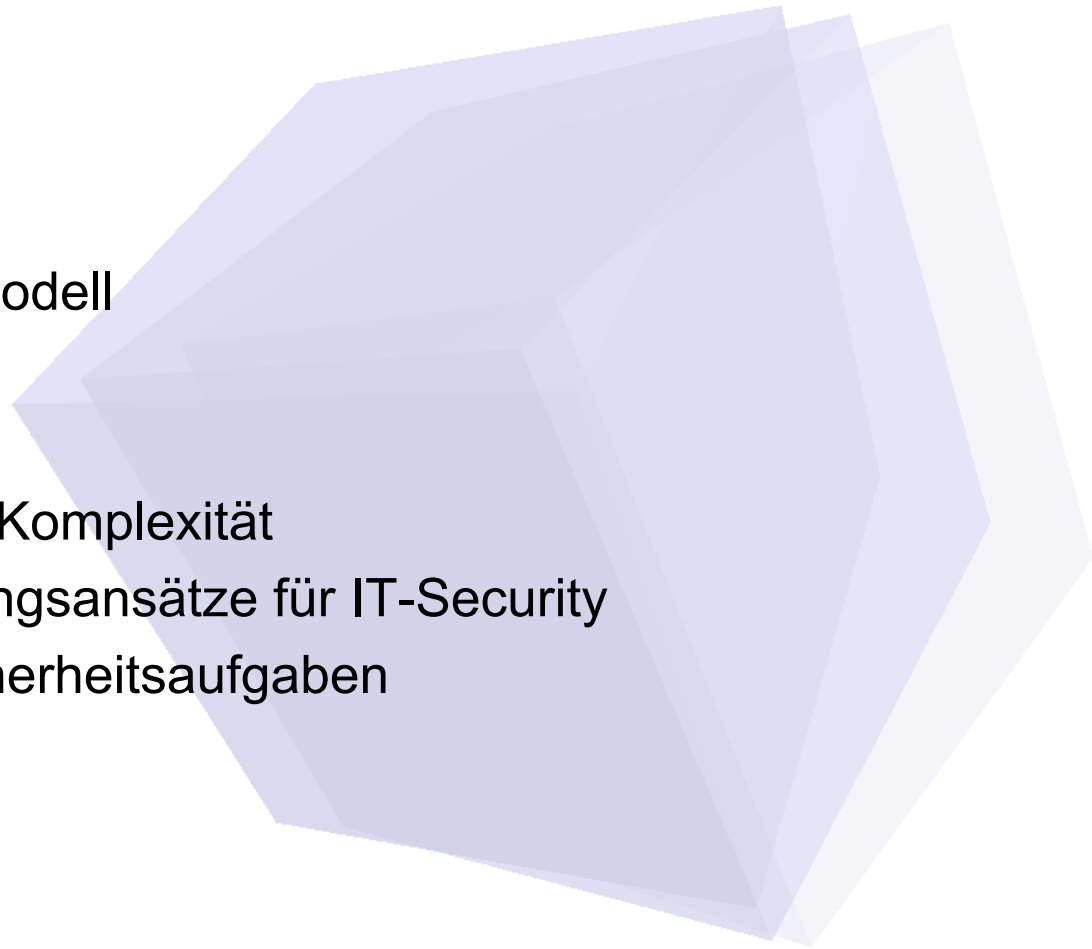
Prof. Dr. B. M. Hämmerli  
E-Mail: [bmhaemmerli@hta.fhz.ch](mailto:bmhaemmerli@hta.fhz.ch)

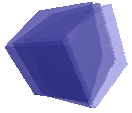




## Inhalt

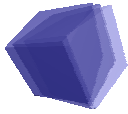
- ❖ Begrüssung
- ❖ Zusammenarbeitsmodell
- ❖ Wer ist der Akteur
- ❖ Was ist Sicherheit
- ❖ Verantwortung und Komplexität
- ❖ Verschiedene Lösungsansätze für IT-Security
- ❖ Delegieren von Sicherheitsaufgaben
- ❖ Schlussfolgerungen
- ❖ Fragen





## Begrüßung I

- ❖ Weshalb diese Tagung?
  - Motivation für IT Security, Driver = (Versicherer und Recht)
- ❖ Wer ist der Akteur dieser Tagung?
  - AG Haftung → iur. Tagung (für Grundlagenerarbeitung)
- ❖ Wer hat all die Arbeit geleistet?
  - Vorstand + Feen im Hintergrund
- ❖ Übersicht Nachmittagsprogramm?
  - Nächste Seite



## Begrüßung II

Einführung, Ing. B. Hämmerli  
IT Risiken beim Bund, Ing. P. Trachsel

### Diskussionsforen zur Haftung

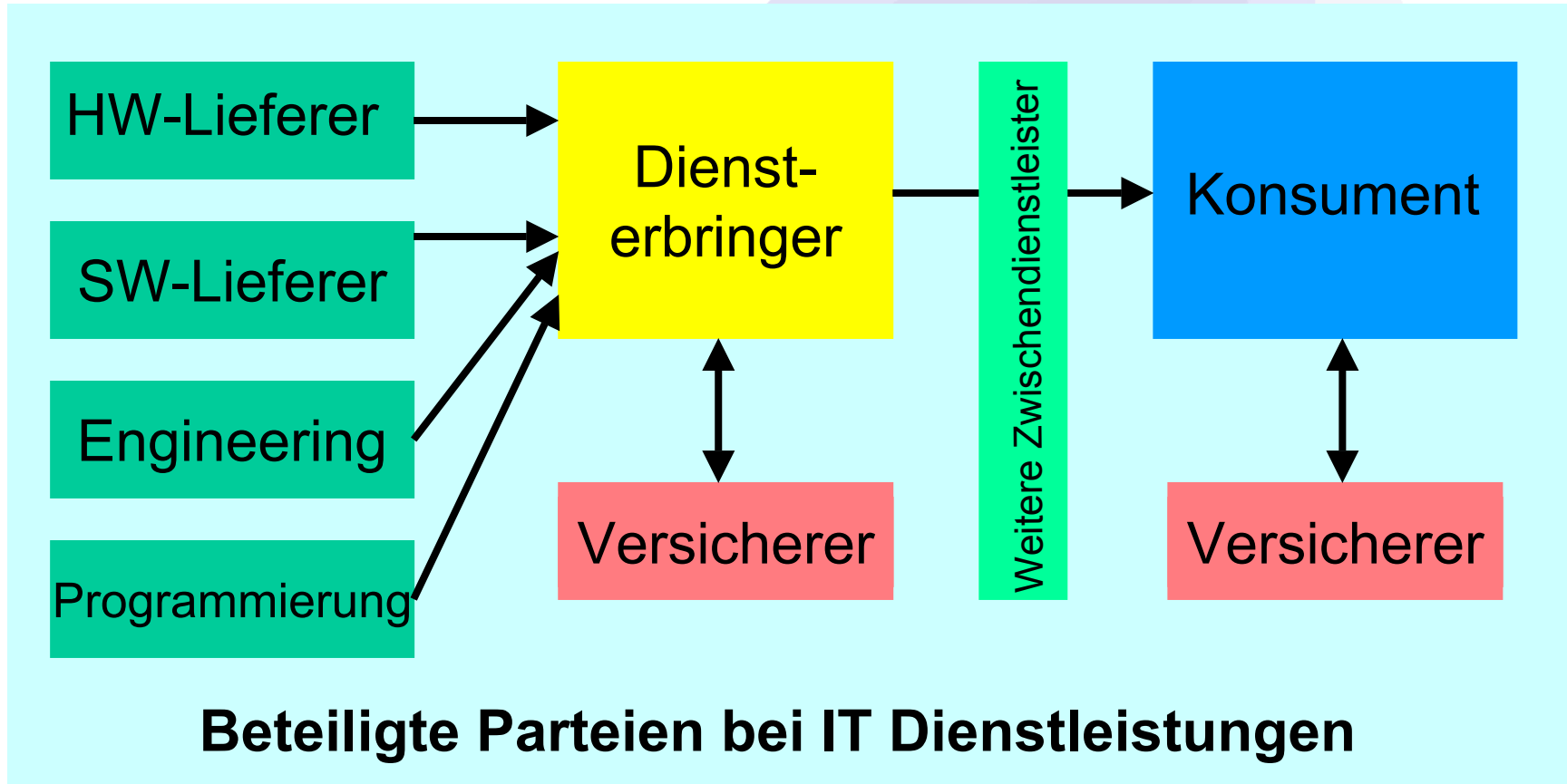
Produkte  
HW- & SW

Dienst-  
leistungen

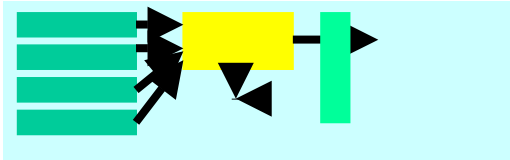
Versicherung  
Risk Controlling

Erarbeitete Resultate aus den Foren

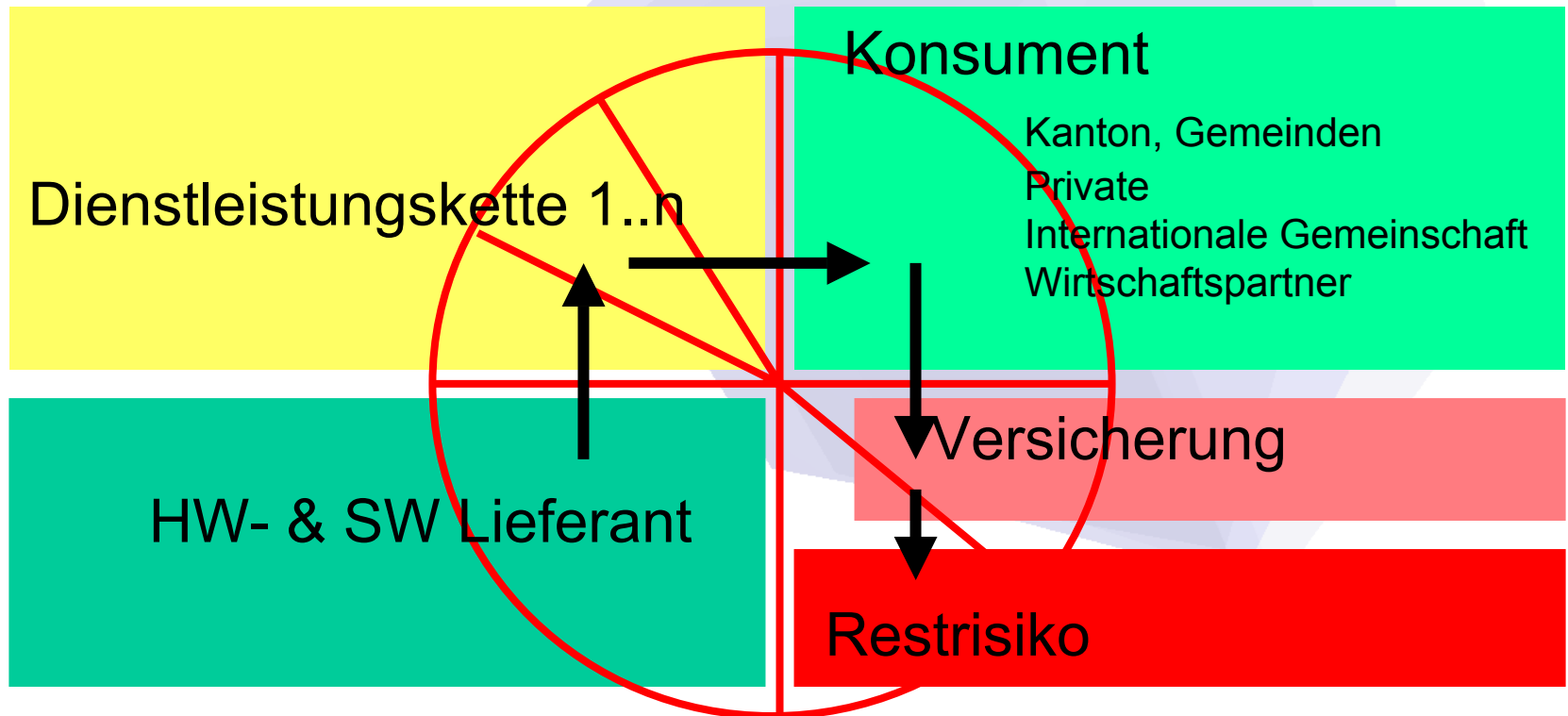
## Zusammenarbeitsmodell I

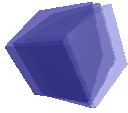


## Zusammenarbeitsmodell II Prozesskette für Dienstleistungserbringung



### Beteiligte Parteien bei IT Dienstleistungen





## Zusammenarbeitsmodell III

### Fragen und Risiken in der Prozesskette

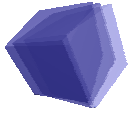
Spezifikation von Dienstleistungen

- ❖ Dienstqualität (SLA Service Level Agreement)
- ❖ Analyse der Risiken
- ❖ Regelung der Haftung bei Verlusten an:
  - Produktionszeit
  - nicht gemachten Geschäften (Opportunität)
  - Wiederherstellung
  - etc.

## Wer ist der Akteur?

Grundsätze aus „Ingenieursicht“

- ❖ Jeder sollte für sein Handeln verantwortlich sein
  - ❖ Daraus ergibt sich ein System aus der Summe der Teile
  - ❖ Das System ist mehr als die Summe aller Teile!
    - Schnittstellen
    - Vollumfassendes Testen und Prüfen komplexer schlecht strukturierter Systeme nicht möglich
    - Integration und Kombinationen von Dienstleistungen:  
HW->OS->Communication->Middleware->Applikationen  
im verteilten Netzwerk
    - Personen, die das System bedienen
    - Organisationsformen
  - ❖ Vertrauen vs. Verantwortung, Enabling vs. Kontrolle
- Schluss:** Akteuransatz versagt!



## Was ist Sicherheit?

### ❖ Betroffene Eigenschaften:

- Verfügbarkeit, ok.
- Vertraulichkeit, ??
- Integrität, heute nur punktuell ein Thema
- Authentizität, die Herausforderung
- Verbindlichkeit, endlich nachvollziehbar, beweisbar und revidierbar!

### ❖ Produktion der Sicherheit:

- Minimieren von Verlusten mit minimalem Einsatz, mit Technologien, Weisungen, Organisation/Strukturierungen, Verantwortlichkeiten, Ausbildung/Sensibilisierung



## Verantwortung und Komplexität

Komplexität:

- ❖ Sicherheit in komplex strukturierten Systemen (technisch, organisatorisch, personell, örtlich) kann nicht vollumfassend geregelt werden.
- ❖ Verschiedene Ansätze:
  - Abstreiten des Themas (aus Investitionsgründen)
  - Best Practice -> COP -> ISO 17799
  - Techniker / Organisatoren / Chefs / Prozessowner / Sicherheitsverantwortliche / Revisoren / Controller

**Schluss:** Ab einer bestimmten Komplexität kann es nur individuelle und spezifische Lösungen geben! Analogien und Beispiele sind hilfreich! Flexibilität für die Erneuerung ist gefragt.

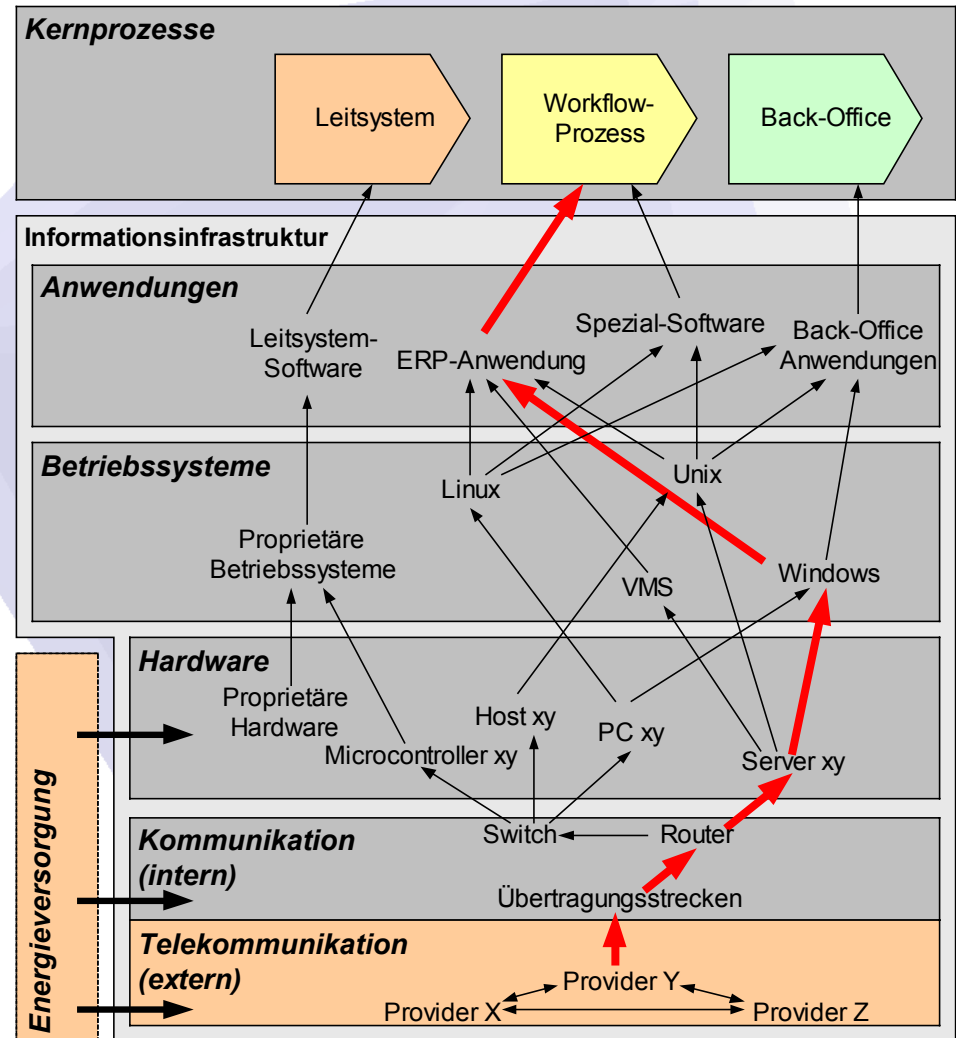


## Verschiedene Lösungsansätze für IT-Security I

1. IT-Security kann mit Technologien gelöst werden.  
(zu Beginn der 90-er Jahre falliert)
2. Lösung mit einem Sicherheitsbeauftragten  
(organisatorische Lösung, ist OK, löst aber das Problem nicht ganz vollständig, Kompetenz, Ressourcen und Weisungsproblem in der Ausführung)
3. Sicherheit ist Chefsache!  
(stimmt, löst aber das Problem auch nicht vollständig. Besser als 2., weil Geld und Verantwortung klar sind)
4. Businessprozesse müssen gesichert werden.  
(Guter Ansatz für eine adäquate Sicherheit. Problem: die Verknüpfung und Abhängigkeiten zwischen Prozessen.)
5. 1-4 kombiniert mit einer Sicherheitsarchitektur

# Verschiedene Lösungsansätze für IT-Security II

Businessprozessmodell:





## Verschiedene Lösungsansätze für IT-Security III

Businessprozessmodell:

- ❖ Erfordert sehr viele Abmachungen (Verträge)  
(Jeweils zwischen jeder zuständigen Stelle)
- ❖ Sehr geeignet für existentielle kritische Infrastrukturen
- ❖ Komplexität kann mit einer **Gesamtsicherheitsarchitektur** teilweise gelöst werden
- ❖ Prozessverantwortliche brauchen Prozesskenntnisse  
(Muss Risiken kenn (vom Fach sein), allgemeiner Manager genügt nicht! Unternehmergeist)



## Delegieren von Sicherheitsaufgaben

Kann die Produktion von Sicherheit ausgelagert werden?

Beispiele:

- Feuerwehr, Polizei, Armee, Securitas
- Telefon, Strom, Strassenverkehr

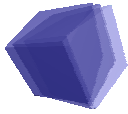
Trends für KMU:

- Sicherheit in einigen Sparten ist zu komplex, um diese selbst herzustellen, Managed Security Services
- Sicherheit aus der Box (die Forschung strengt sich in bestimmten Bereichen für Vereinfachungen an!)

Heute gibt es externe Sicherheitslösungen für:

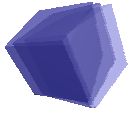
- Firewall, Intrusion Detection, Viren etc.
- Zur Authentisierung (Zertifikate)
- Zur Verfügbarkeit (Backuprechenzentren)
- weitere Bereiche werden kommen

→ [www.fgsec.ch](http://www.fgsec.ch) Tagung vom 18. Nov. 03



## Schlussfolgerung I

- ❖ Risk Assessment in komplexen Systemen muss architekturell und prozessorientiert angegangen werden, und sollte in ein Haftungsassessment führen.
- ❖ Verschiedene Lösungsansätze für IT-Security sind ergänzend und aufbauend zueinander Zeittrends gewesen und müssen in eine Gesamtarchitektur integriert werden.
- ❖ Delegieren von Sicherheitsaufgaben wird aus Kostengründen in verschiedenen Bereichen unumgänglich.
- ❖ Sicherheit wird entscheidend im Wettbewerb der Zukunft sein!



## Schlussfolgerungen II

### ❖ Mein Wunsch:

- Klarheit auf dem Weg vom Risk Assessment zum Haftungsassessment.
- Dadurch Förderung der Sicherheit auf allen Ebenen in eine zweckorientierte, lösungsangepasste und bedarfsgerechte Sicherheit.
- Vermeiden von Konfliktfällen

