Kollaboratives IT-Sicherheitsmanagement auf Basis von BSI-Grundschutz

Hannes Federrath, Christoph Gerber

Sicherheit in Verteilten Systemen

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Was ist IT-Sicherheitsmanagement?

- ~ beschreibt eine systematische Vorgehensweise zur Absicherung des Informationsverbundes eines Unternehmens oder einer Behörde

- Typische Aufgaben
  - Entwicklung eines Sicherheitskonzeptes
  - Identifizierung und Realisierung angemessener Sicherheitsmaßnahmen
  - Schulung und Sensibilisierung von Mitarbeitern
  - Erhaltung der IT-Sicherheit im laufenden Betrieb

- Abhängigkeit der Unternehmen von IT
  - „Je mehr Funktionen eine Organisation mit Hilfe von IT-Systemen erledigt, umso abhängiger wird sie von der fehlerfreien und verlässlichen Funktion der Systeme."

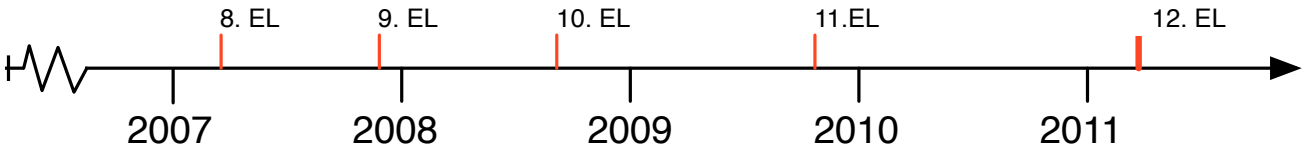
[ScWe07]

BSI-Grundschutz

- Vorgehensmodell zur systematischen Absicherung eines unternehmensweiten Informationssystems

- Vier Standards (BSI 100-1 bis BSI 100-4)
  - beschreiben Einführung und Betrieb eines Informationssicherheitsmanagementsystems (ISMS)
  - Kompatibilität zu internationalen Standards (ISO 27001)

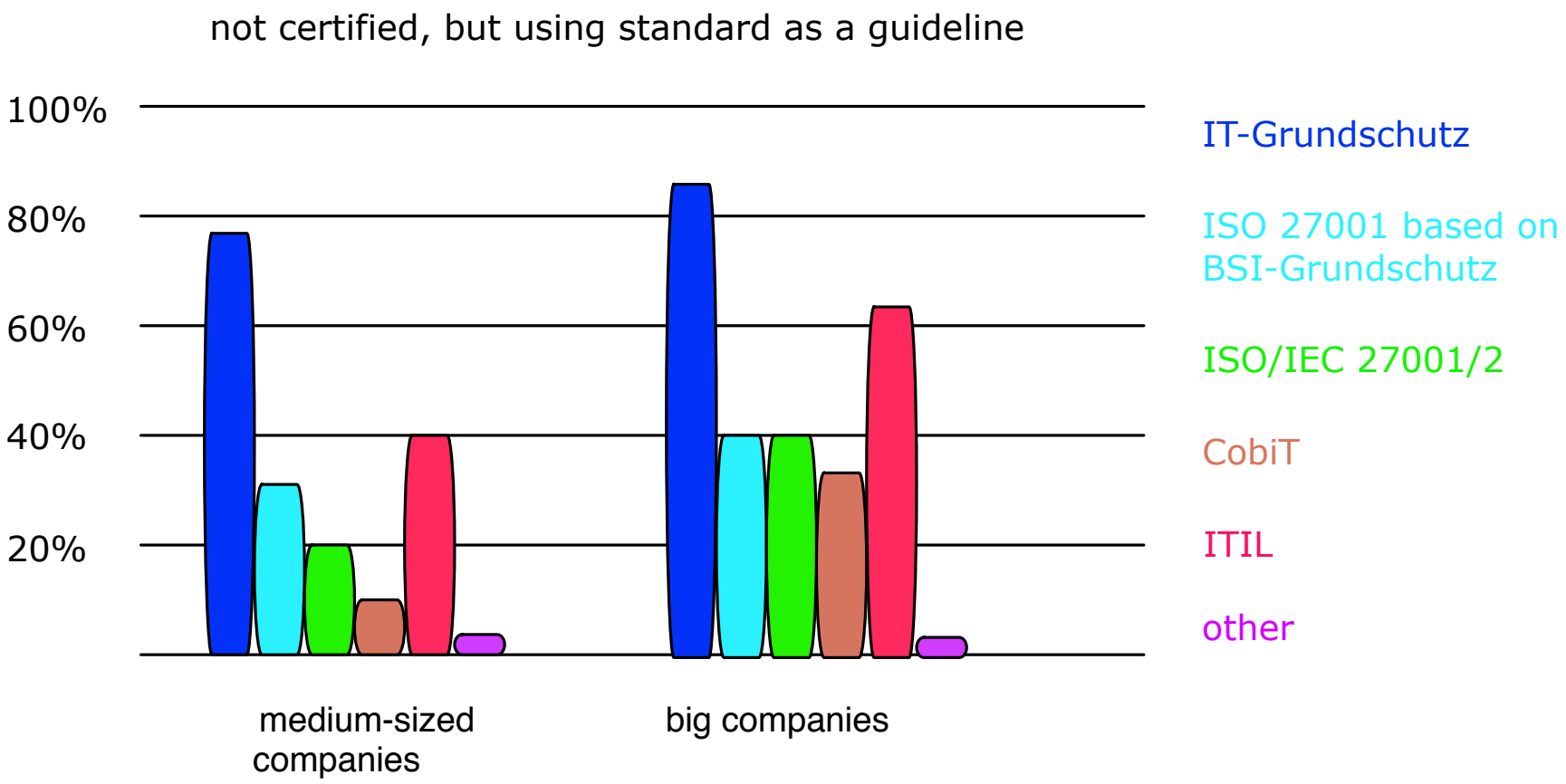
- IT-Grundschutzkataloge
  - Umfassende Sammlung von IT-Sicherheitsmaßnahmen auf operativer Ebene
  - Kontinuierliche Weiterentwicklung



(BSI-Grundschutz: letzte Ergänzungslieferungen)

Wer arbeitet mit BSI-Grundschutz?

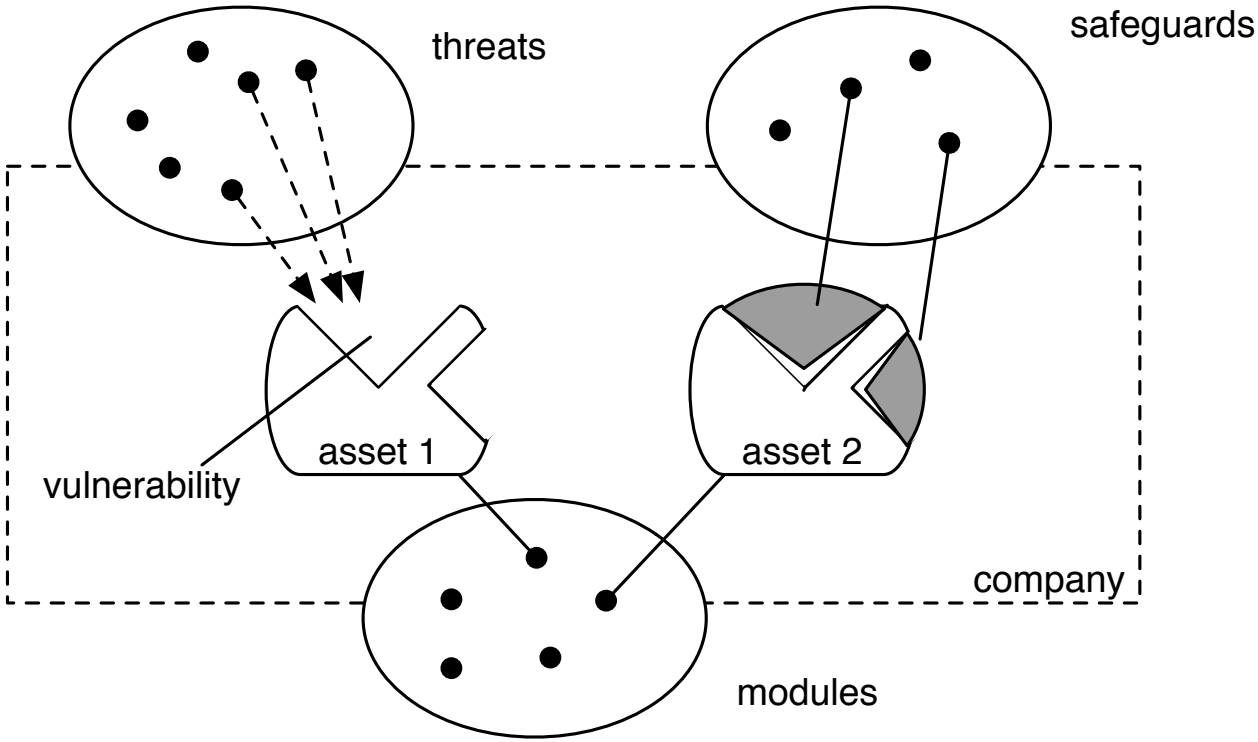
- Behörden und Unternehmen



(cf. Kronschnabel et al. 2011)

BSI-Grundschutz zusammengefasst

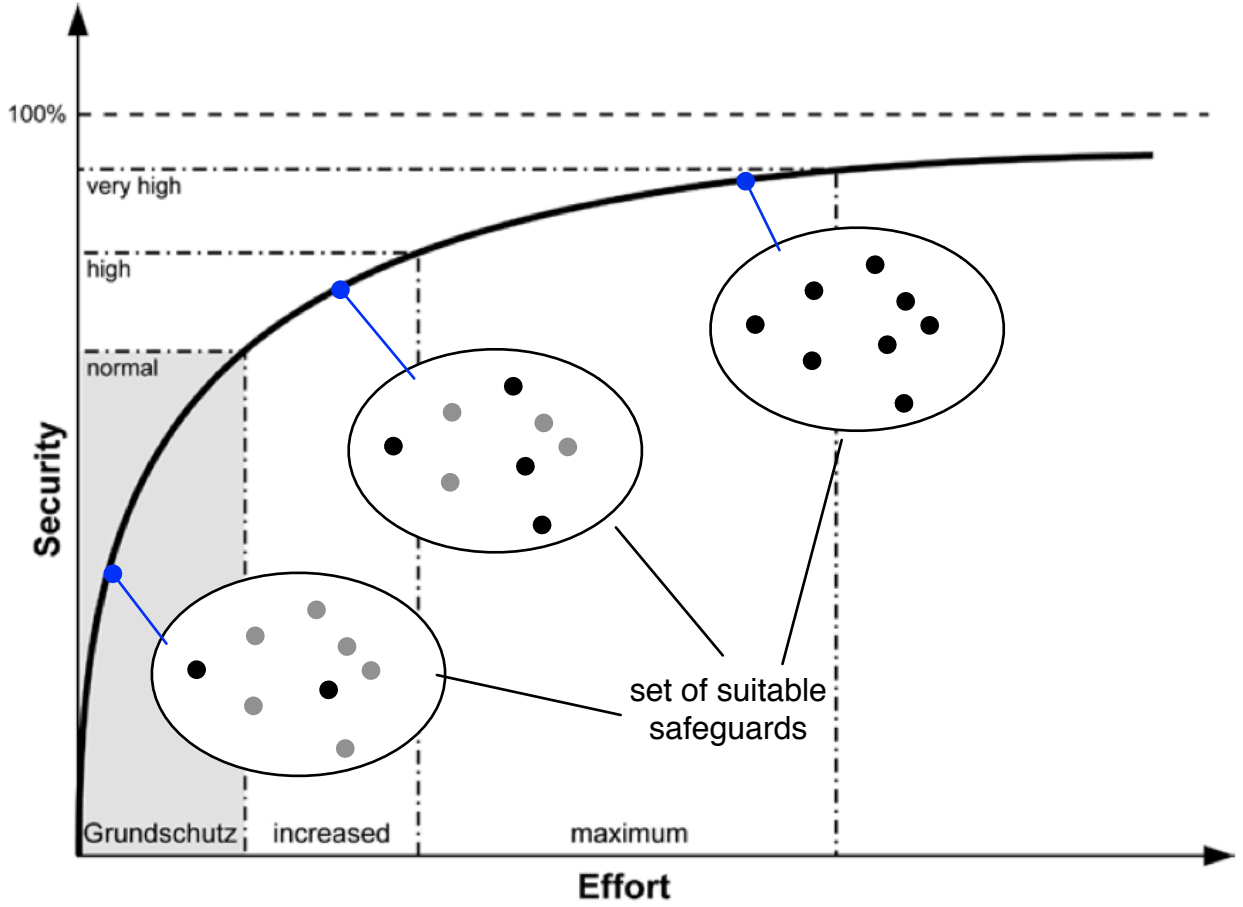
- Modularer Aufbau (Baukastensystem)



(BSI-Grundschutz: Mengendarstellung)

Eine Menge von Maßnahmen für ein best. Sicherheitslevel

- "Wäre es nicht gut zu wissen, welches Maßnahmenbündel für mein Unternehmen das Sicherheitslevel am besten verbessert?"



(BSI 100-2: erreichbare Sicherheitslevels)

Zusammenarbeit erwünscht / Vorteile

- Unternehmen setzen Grundschutz in Eigenregie um
  - Etwa die Hälfte der Unternehmen zieht ein Beratungsunternehmen hinzu
  - Kollaborationswerkzeuge können eine Bereicherung sein

- Statistische Aussagen über die Umsetzung von IT-Sicherheitsmaßnahmen
  - für teilnehmende Unternehmen
  - für das BSI

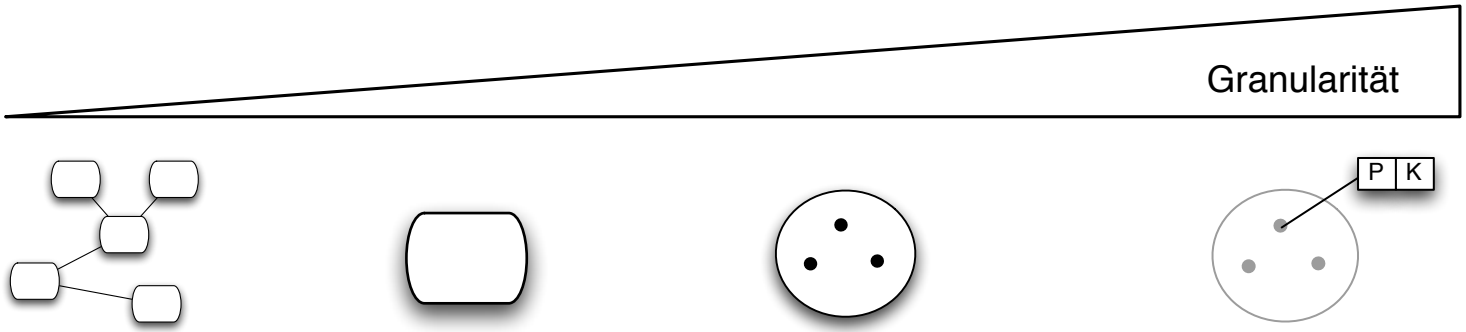
- Erweiterte Plausibilitätskontrolle von Eingabedaten

→ Wichtiger Schritt hin zu einem Entscheidungsunterstützungssystem zur Planung und Realisierung von IT-Sicherheitsmaßnahmen

Wer tauscht bereits Daten im Sicherheitsbereich

- Umsetzungsplan KRITIS
  - Plan zum Schutz deutscher Informationsinfrastrukturen (BSI)
- CarmentiS
  - Basisinfrastruktur für ein deutsches IT-Frühwarnsystem (CERT-Verbund)
- PS3IO
  - Plattform zum überbetrieblichen Austausch von Informationen zu Informationssicherheitsvorfällen (Nowey 2011)
- Practical Privacy-Preserving Benchmarking
  - Sicherer Vergleich von Unternehmen hinsichtlich im Vorfeld erhobener Key Performance Indicators (KPIs) (Kerschbaum 2008)

Datenquellen für Unternehmensvergleiche im BSI-GS

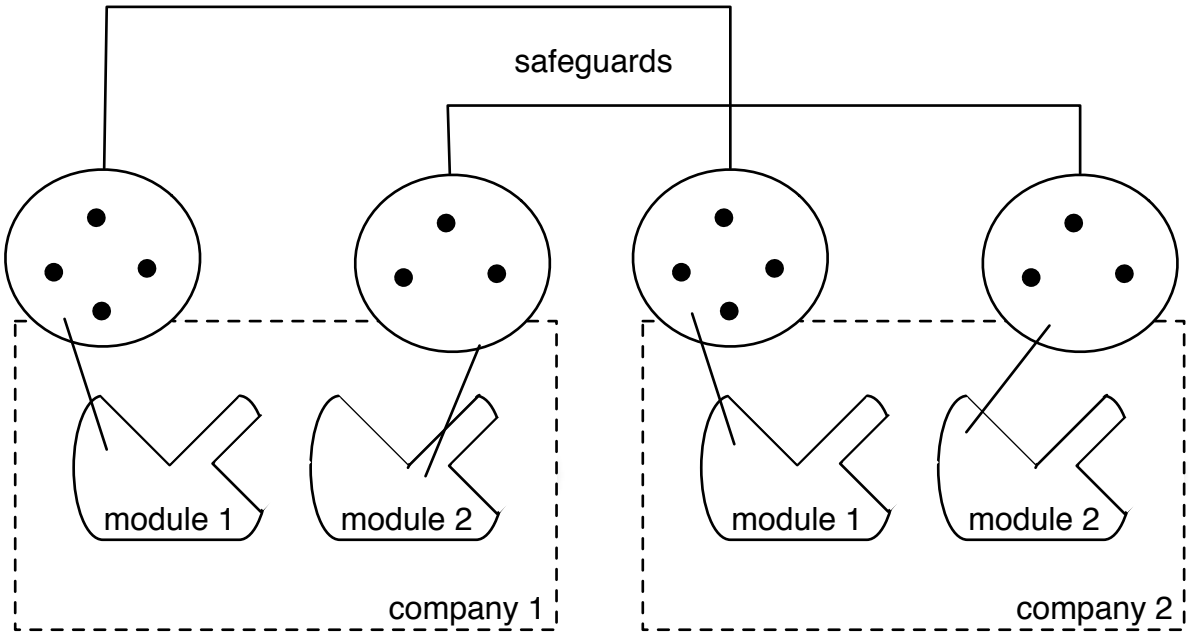


Informations-verbund	**Bausteine**	**Maßnahmen**	**Prüf-/ Kontrollfragen**	
• beliebig; unternehmens-abhängig	• 85 Bausteine	• 1234 Maßnahmen	• 1927 Kontrollfragen • 1143 Prüffragen	**Anzahl**
• Verlinkungs-struktur • Zusammen-fassung zu Gruppen • Anzahl Geräte, Nutzer, Mitarbeiter, ...	• Namensgebung von Assets • Schutzbedarfe	• Umsetzungsgrad von Maßnahmen • Begründung der Umsetzung	• Beantwortung von Fragen zu Einzelzuständen der Assets	**Daten-quellen**

(Zahlen aus der 11. Ergänzungslieferung)

Lernen durch Vergleiche mit anderen Sicherheitskonzepten

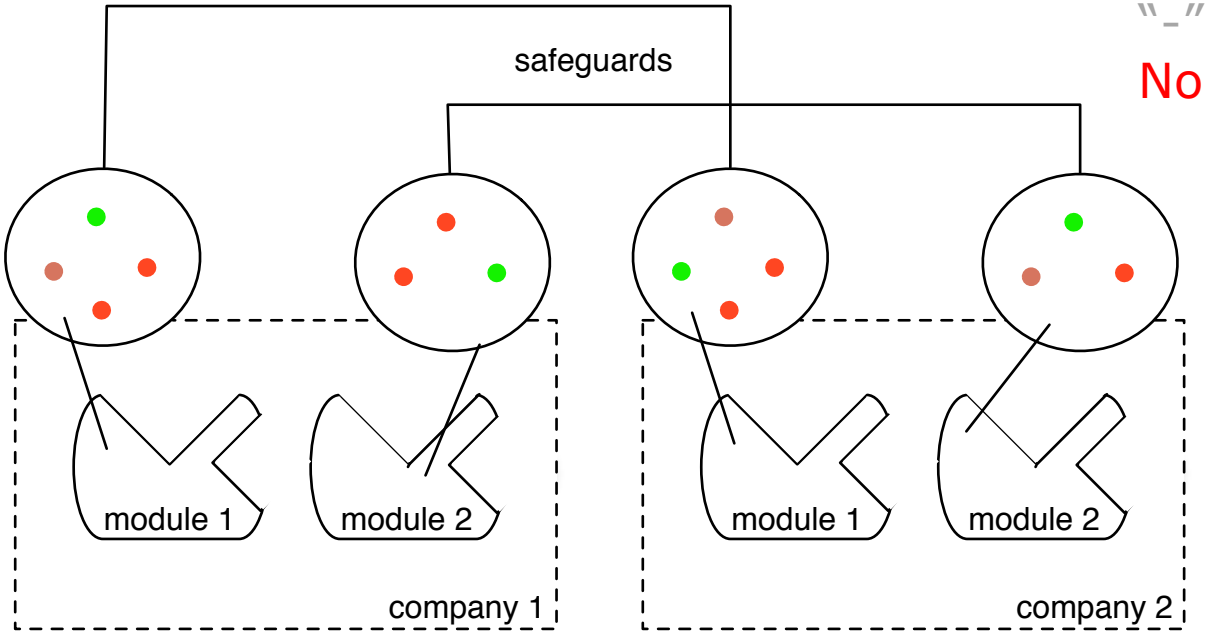
- Unternehmensvergleich auf Maßnahmenebene



Lernen durch Vergleiche mit anderen Sicherheitskonzepten

- Unternehmensvergleich auf Maßnahmenebene

Possible Answers:
Yes
Partly
"-"
No



safeguards

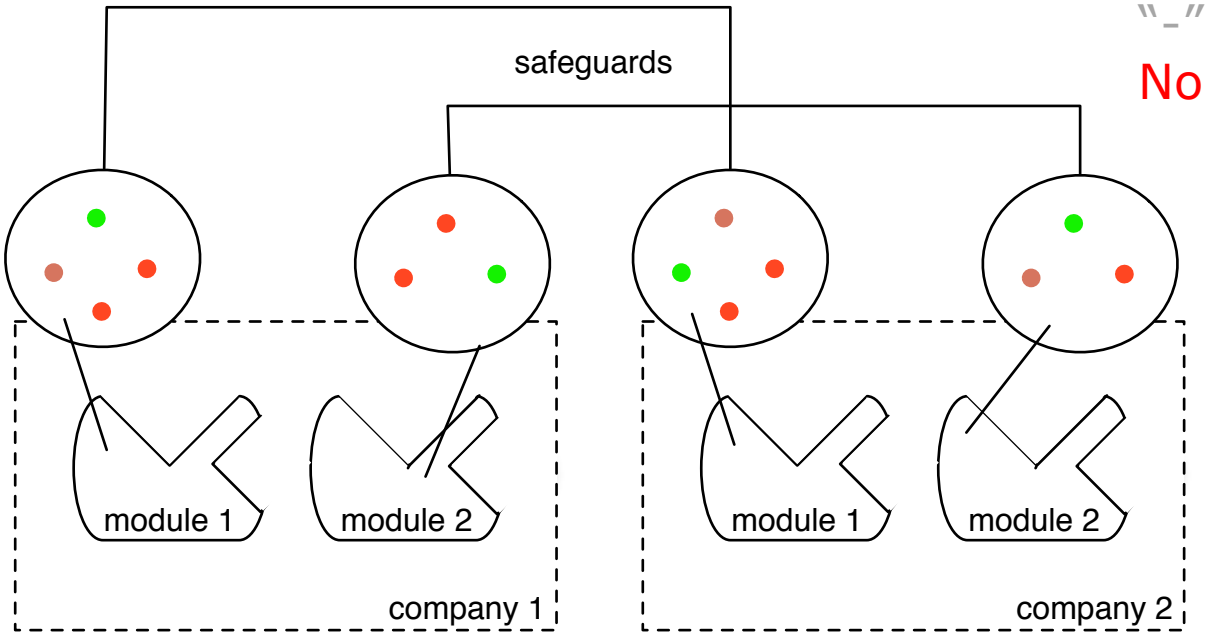
	S1,	S2,	S3,	S4
m1{	yes,	no,	no,	partly}
m2{	no,	yes,	no	}

	S1,	S2,	S3,	S4
m1{	partly,	no,	no,	yes}
m2{	yes,	no,	partly	}

Lernen durch Vergleiche mit anderen Sicherheitskonzepten

- Unternehmensvergleich auf Maßnahmenebene

Possible Answers:
Yes
Partly
"-"
No

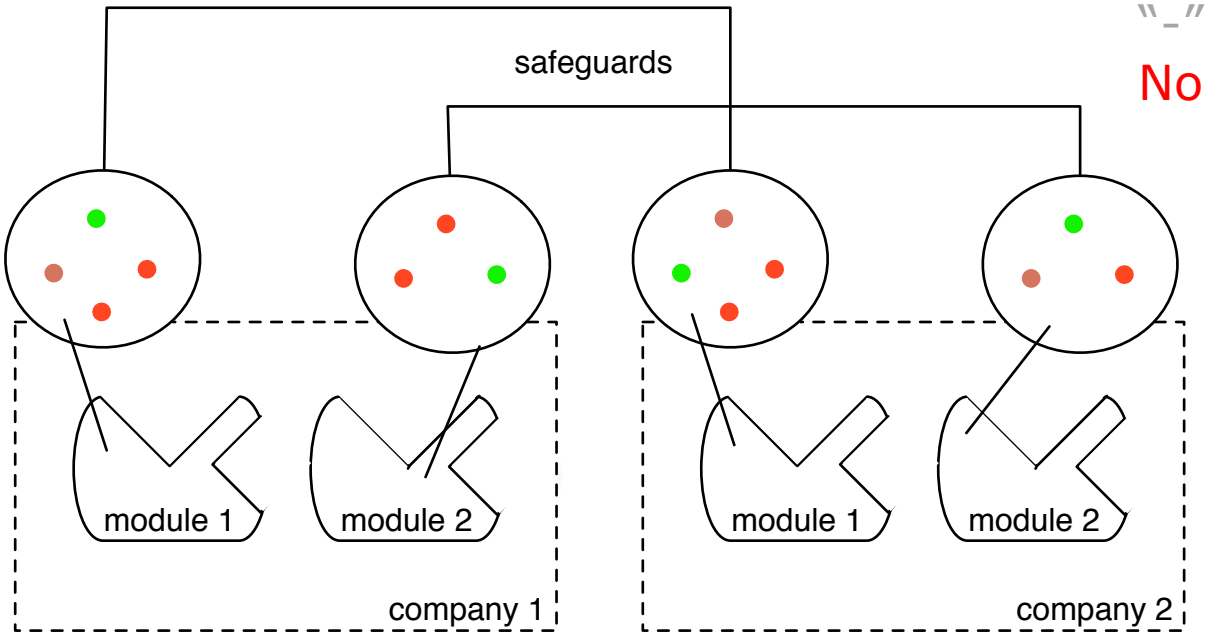


safeguards	S1,	S2,	S3,	S4		S1,	S2,	S3,	S4	
similarity	m1{yes,	no,	no,	partly}		m1{partly,	no,	no,	yes}	=0.5
	m2{no,	yes,	no	}		m2{yes,	no,	partly	}	=0.0

Lernen durch Vergleiche mit anderen Sicherheitskonzepten

- Gewichtetes Ähnlichkeitsmaß

Possible Answers:
Yes ≙ 2
Partly ≙ 1
"-" ≙ 0
No ≙ -1



safeguards S1, S2, S3, S4 S1, S2, S3, S4

similarity
m1{yes, no, no, partly} m1{partly, no, no, yes} =0.5
m2{no, yes, no } m2{yes, no, partly } =0.0

similarity
m1{yes, no, no, partly} m1{partly, no, no, yes} =0.83
m2{no, yes, no } m2{yes, no, partly } =0.08

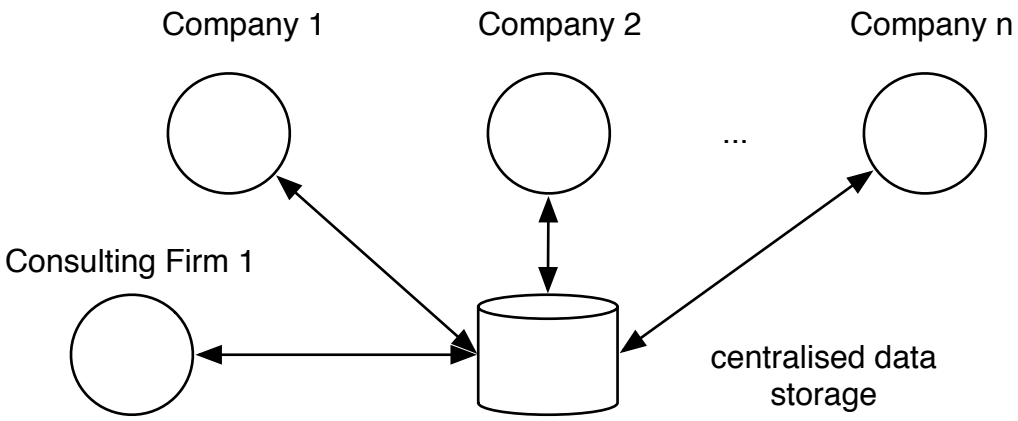
Lernen durch Vergleiche mit anderen Sicherheitskonzepten

- Vergleich von 9 Gruppen hinsichtlich der Umsetzung eines bestimmten Bausteins innerhalb einer Fallstudie

	Gruppe 1	Gruppe 2	Gruppe 3	Gruppe 4	Gruppe 5	Gruppe 6	Gruppe 7	Gruppe 8	Gruppe 9
Gruppe 1		0,5	0,5	0,5	0,6	0,55	0	0,65	0,5
Gruppe 2			0,55	0,5	0,55	0,45	0	0,55	0,5
Gruppe 3				0,6	0,65	0,55	0,05	0,55	0,8
Gruppe 4					0,75	0,65	0,05	0,65	0,5
Gruppe 5						0,85	0	0,8	0,6
Gruppe 6							0	0,8	0,5
Gruppe 7								0	0,15
Gruppe 8									0,5
Gruppe 9									

Ein System zur Sammlung von Daten im Grundschutz

- Client-Server-Modell



- Kernanfroderungen
  - Nützlichkeit
  - Mehrseitige Sicherheit
  - Benutzbarkeit

Nützlichkeit

- Informationsaustausch muss vorteilsbehaftet für teilnehmende Unternehmen sein
  - wirtschaftliche Auswahl von IT-Sicherheitsmaßnahmen
  - Unterstützung in der Realisierungsplanung
  - erweiterte Validitätstests bei der Dateneingabe

- Probleme bei Vergleichbarkeit von Unternehmen
  - Auswahl und Aufbereitung geeigneter Daten
    - z.B. unterschiedliche Granularität von Sicherheitsmaßnahmen
  - Vergleichbarkeit zwischen Unternehmen
    - Unternehmen sind unterschiedlich!
    - Unternehmen können Sachverhalte unterschiedlich interpretieren!
  - ...

Nützlichkeit

Unternehmen werden nur teilnehmen, wenn es nützlich ist für sie!

Mehrseitige Sicherheit

- Vertraulichkeit als vordringliches Entwurfsziel
  - Pseudonymisierung
  - Anonyme Serververbindungen
  - Reduktion von identifizierenden Merkmalen in Freitextfeldern
  - ...

- Beispiel: Interessenskonflikt im Geben und Erhalten von Informationen
  - Teilnehmer wollen anonym bleiben und ihre eigenen Informationen so gut es geht schützen

    vs.
  - Daten die von anderen Unternehmen stammen sollen repräsentativ und korrekt sein

  - Führt zu Problemen wie
    - free-riding
    - truth-telling

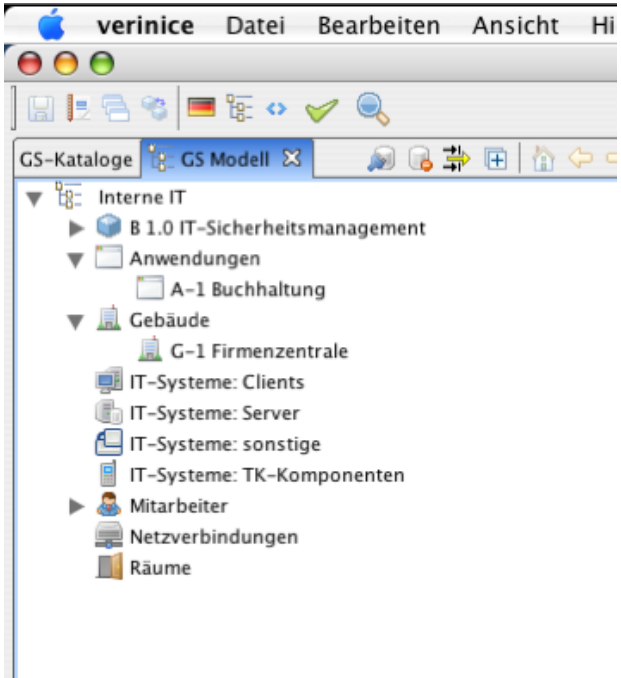
Mehrseitige Sicherheit

Unternehmen werden nur teilnehmen, wenn es sicher ist für sie!

Benutzbarkeit

- IT-Sicherheit als Sekundärfunktion innerhalb von Unternehmen
  - Aufwand für Datenerhebung geringhalten

- IT-Grundschutz innerhalb von Unternehmen wird oft durch Software-Werkzeuge unterstützt
  - GSTOOL
  - verinice



→Bestehende Datenquellen nutzen!

Benutzbarkeit

Unternehmen werden nur teilnehmen, wenn es leicht handhabbar ist für sie!

Zusammenfassung

- Grundschutz als etablierter Standard im Sicherheitsmanagement
- Unternehmensübergreifender Datenaustausch als Möglichkeit bessere Entscheidungen über Sicherheitsinvestitionen zu treffen
- Mehrseitige Sicherheit als wichtige Kernanforderung für ein System zum Datenaustausch
- Unterstützung willkommen ☺

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Vogt-Kölln-Straße 30
D-22527 Hamburg

Christoph Gerber
E-Mail gerber@informatik.uni-hamburg.de
Telefon +49 40 42883 2347
http://svs.informatik.uni-hamburg.de