Mehrseitige Sicherheit 2.0

Andreas Pfitzmann

TU Dresden, Fakultät Informatik, D-01062 Dresden
Nöthnitzer Str. 46, Raum 3071
Tel.: 0351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

Ziele meines Vortrags

- Tiefes Grundverständnis für IT-Sicherheit wecken
- Günter Müllers Beiträge hierzu als Wissenschaftler und Mensch würdigen
- Nächste fachliche Herausforderungen skizzieren

Gliederung

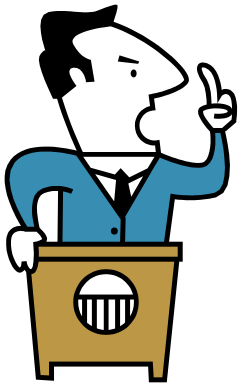
- Sicherheit
  - Was?
  - Für wen?
  - Gegen wen?
- Mehrseitige Sicherheit
  - Klassische Defs
  - Klassische Schutzziele
- Mehrseitige Sicherheit 2.0
  - Communities: Konsistenz + Fairness
  - Menschen reifen: Zeitverläufe
- Ausblick
  - Was forschen?
  - Was lehren?
  - Was leben?

Sicherheit

- Was?
  - Keine (oder zumindest möglichst wenig) Auswirkungen von Gefahren
- Für wen?
  - Für die Guten
- Gegen wen?
  - Gegen die Bösen

IT- Sicherheit

- Was?
  - Keine (oder zumindest möglichst wenig) Auswirkungen von Gefahren
  - CIA = Confidentiality, Integrity, Availability
- Für wen?
  - Für die Guten
  - Für den Betreiber des Systems
- Gegen wen?
  - Gegen die Bösen
  - Gegen den Rest der Welt



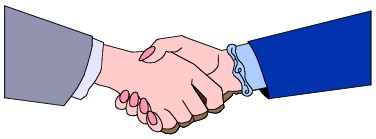
Stand der öffentlichen Wahrnehmung
vor Günter Müllers Engagement

Mehrseitige Sicherheit

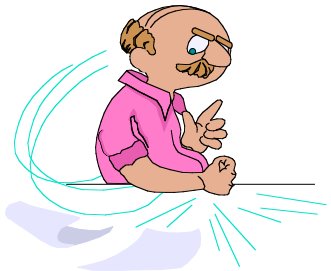
- Jeder Beteiligte hat eigene Sicherheitsinteressen.

- Jeder Beteiligte kann seine Sicherheitsinteressen formulieren.

- Konflikte werden erkannt und Lösungen ausgehandelt.



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.

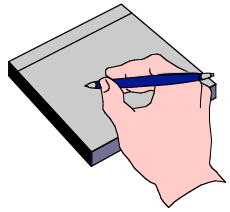


Sicherheit mit minimalen Annahmen über andere

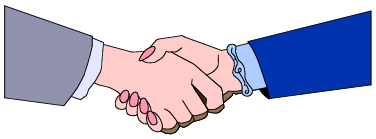
Mehrseitige Sicherheit (2. Version)

- Jeder Beteiligte hat eigene Interessen.

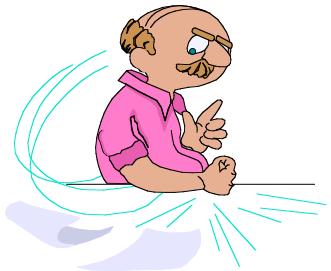
- Jeder Beteiligte kann seine Sicherheitsinteressen formulieren.



- Konflikte werden erkannt und Lösungen ausgehandelt.



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.



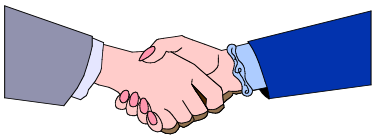
Sicherheit mit minimalen Annahmen über andere

Mehrseitige Sicherheit (3. Version)

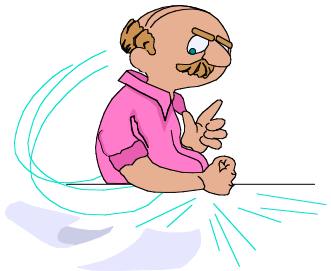
- Jeder Beteiligte hat eigene Interessen.

- Jeder Beteiligte kann seine Sicherheitsinteressen formulieren.

- Konflikte werden erkannt und Lösungen ausgehandelt.



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen. Grenzen der Durchsetzbarkeit betreffen alle Beteiligten in gleicher Weise.



Sicherheit mit minimalen Annahmen über andere

Mehrseitige Sicherheit (4. Version)

- Jeder Beteiligte hat ...

- Jeder Beteiligte kann ...

Immanuel Kants Imperativ angewandt auf Sicherheit

Schutzziele: Sortierung

	Inhalte	Umfeld
Unerwünschtes verhindern	Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Erwünschtes leisten	Integrität	Zurechenbarkeit
	Verfügbarkeit	Erreichbarkeit Verbindlichkeit

Schutzziele: Definitionen

Vertraulichkeit: Geheimhaltung von Daten während der Übertragung. Niemand außer den Kommunikationspartnern kann den Inhalt der Kommunikation erkennen.

Verdecktheit: Versteckte Übertragung von vertraulichen Daten. Niemand außer den Kommunikationspartnern kann die Existenz einer vertraulichen Kommunikation erkennen.

Anonymität: Nutzer können Ressourcen und Dienste benutzen, ohne ihre Identität zu offenbaren. Selbst der Kommunikationspartner erfährt nicht die Identität.

Unbeobachtbarkeit: Nutzer können Ressourcen und Dienste benutzen, ohne daß andere dies beobachten können. Dritte können weder das Senden noch den Erhalt von Nachrichten beobachten.

Integrität: Modifikationen der kommunizierten Inhalte (Absender eingeschlossen) werden durch den Empfänger erkannt.

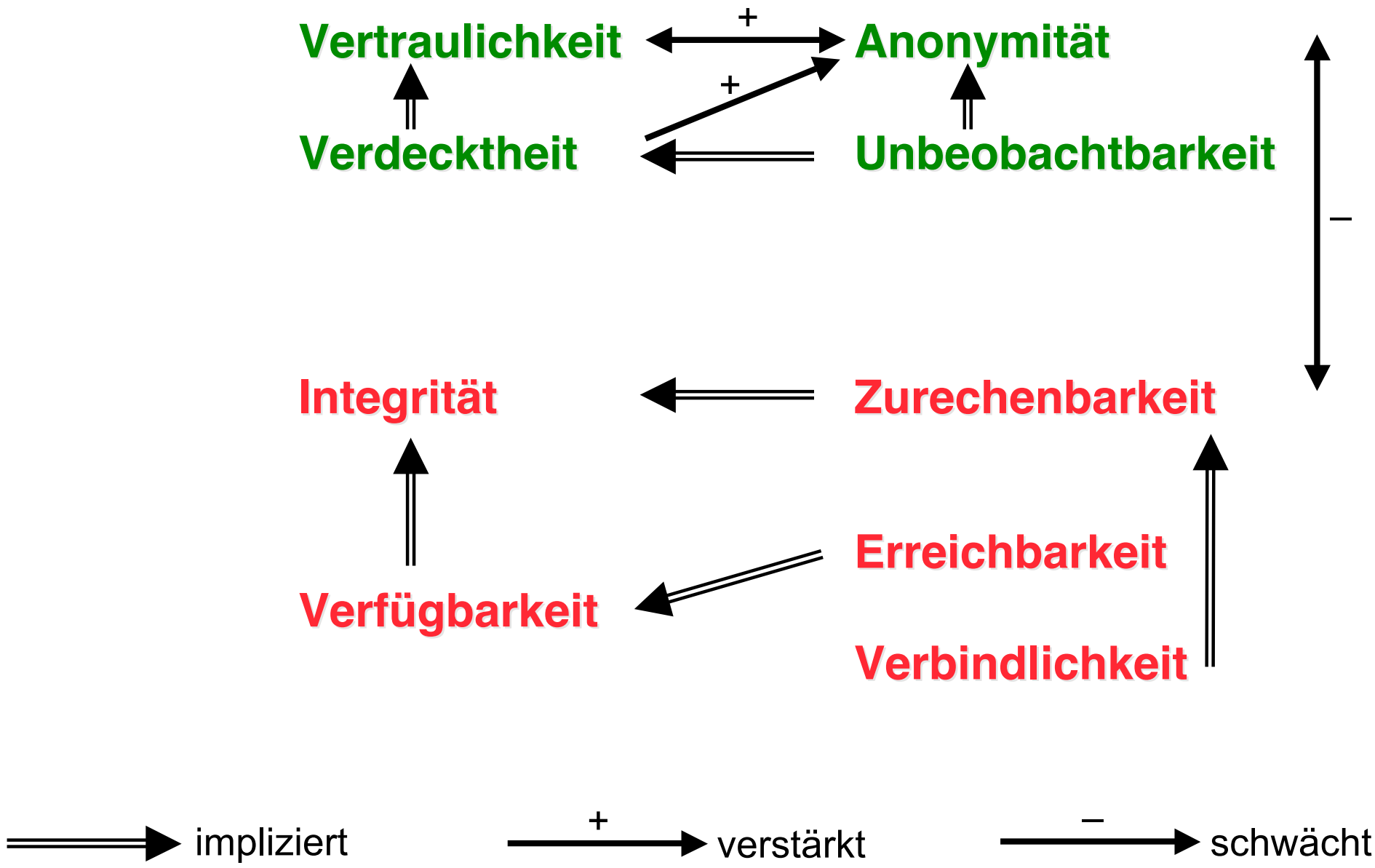
Zurechenbarkeit: Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden.

Verfügbarkeit: Nutzbarkeit von Diensten und Ressourcen, wenn ein Nutzer sie benutzen will.

Erreichbarkeit: Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht.

Verbindlichkeit: Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.

Wechselwirkungen zwischen Schutzzielen



Communities: Konsistenz + Fairness

Neue Anwendungen, u.a. für Communities, erfordern weitere Schutzziele:

- **Konsistenz**, d.h. Mengen von Nutzern erhalten gleichzeitig das Gleiche oder können zumindest erkennen, wenn dies nicht der Fall ist.
- **Fairness**, d.h. Mengen von Nutzern können Ressourcen und Dienste in gleichberechtigter, möglichst sogar gleicher Weise nutzen.

Konsistenz und Fairness können einerseits als ***Meta-Schutzziele*** interpretiert werden, die (nahezu) alle Schutzziele erweitern, oder andererseits an ihren wichtigsten Stellen in der Schutzzielsystematik als ***konkrete weitere Schutzziele*** eingeführt werden.

Schutzziele: Definitionen

Vertraulichkeit: Geheimhaltung von Daten während der Übertragung. Niemand außer den Kommunikationspartnern kann den Inhalt der Kommunikation erkennen.

Verdecktheit: Versteckte Übertragung von vertraulichen Daten. Niemand außer den Kommunikationspartnern kann die Existenz einer vertraulichen Kommunikation erkennen.

Anonymität: Nutzer können Ressourcen und Dienste benutzen, ohne ihre Identität zu offenbaren. Selbst der Kommunikationspartner erfährt nicht die Identität.

Unbeobachtbarkeit: Nutzer können Ressourcen und Dienste benutzen, ohne daß andere dies beobachten können. Dritte können weder das Senden noch den Erhalt von Nachrichten beobachten.

Integrität: Modifikationen der kommunizierten Inhalte (Absender eingeschlossen) werden durch den Empfänger erkannt.

Zurechenbarkeit: Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden.

Konsistenz: Senden und Empfangen von Informationen wird auch bei Multicast von allen Beteiligten gleich gesehen und kann auch Unbeteiligten bewiesen werden.

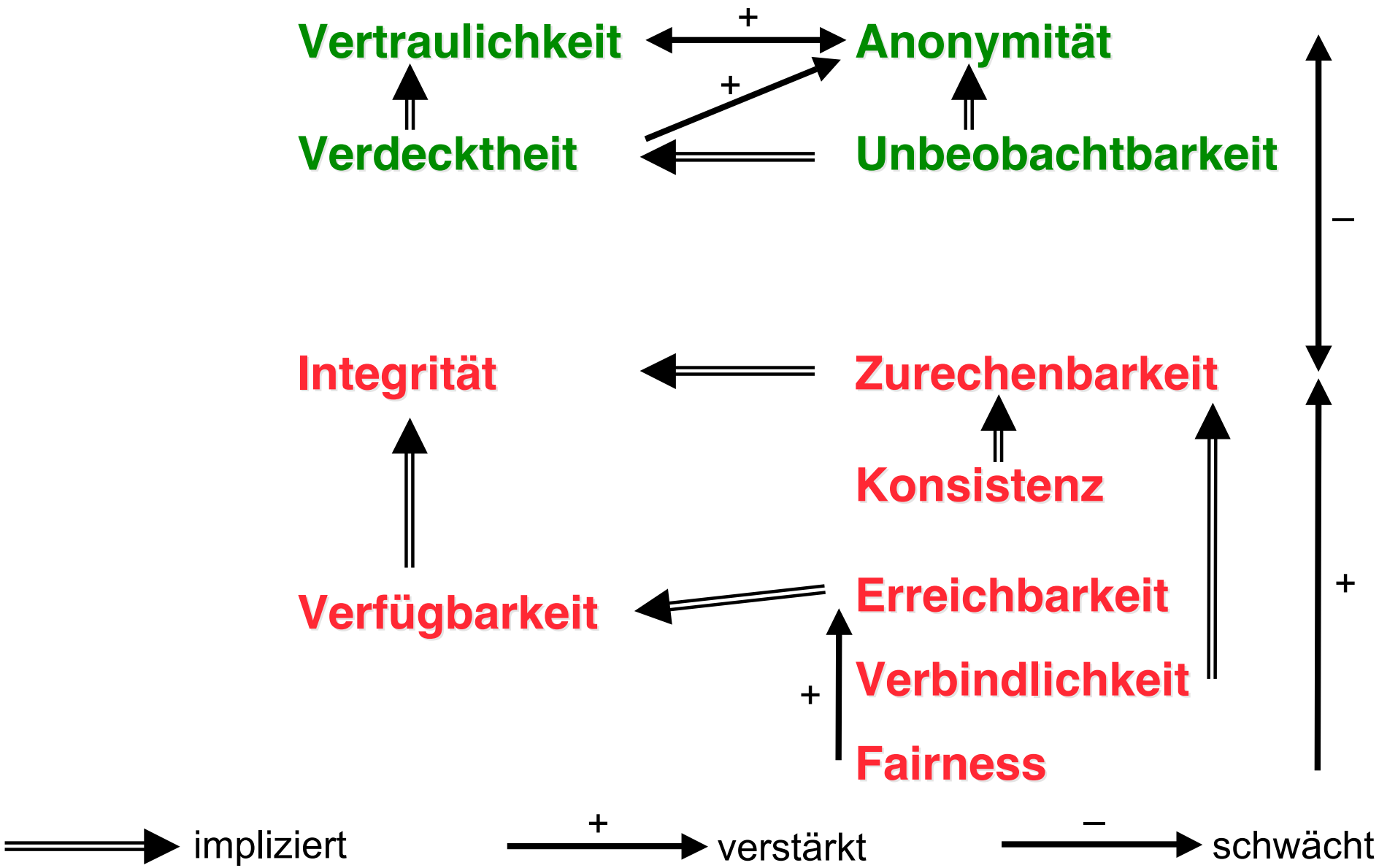
Verfügbarkeit: Nutzbarkeit von Diensten und Ressourcen, wenn ein Nutzer sie benutzen will.

Erreichbarkeit: Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht.

Verbindlichkeit: Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.

Fairness: Benutzung von Ressourcen und Diensten ist allen Nutzern und Maschinen in gleichberechtigter, möglichst sogar gleicher Weise möglich.

Wechselwirkungen zwischen Schutzzielen, zwei zusätzliche



Menschen reifen: Zeitverläufe

- Was, wenn sich Interessen von Menschen ändern?
- Aktuelle Sicherheitsinteressen formulieren.
- Nachverhandeln? Geht nur bzgl. noch vorhandener Daten und wenn die anderen Beteiligten noch zur Verfügung stehen (wollen).
- Durchsetzbarkeit? Anderen Beteiligten Daten „wegnehmen“ ist kaum realisierbar.

Sicherheit mit realistischeren Annahmen über einen selbst

und sodann möglichst schwachen Annahmen über andere

Kompromiss Zeitverläufe

- Zeitverläufe schon von Anfang an formulieren und aushandeln?
- Einfacher als Nachverhandeln, aber gleiche Probleme mit der Durchsetzbarkeit (Daten „wegnehmen“ ist kaum realisierbar).

Ausblick

- Was forschen?
  - Nicht nur Probleme wirklich lösen, sondern auch die wirklichen Probleme lösen
  - Geht nur disziplinenübergreifend
- Was lehren?
  - Ehrlichkeit, Realismus, Rückgrat
  - Grundverständnis für Sicherheit als Sicherheit auch der anderen
  - Problemanalyse und realistische Bewertung von Lösungen
  - Zuallerletzt: Sicherheitsmechanismen
  - Keinesfalls: Patentrezepte
- Was leben?
  - Auch mit den Augen der anderen sehen
  - Ehrliche realistische Problemanalysen verständlich kommunizieren