Gesellschaftliche Strukturen im digitalen Wandel

Vorlesung im Modul 10-201-2333 im Wahlbereich Bachelor der Geistes- und Sozialwissenschaften

Wintersemester 2013/14

Prof. Dr. Hans-Gert Gräbe

http://bis.informatik.uni-leipzig.de/HansGertGraebe

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Interdisziplinarität

Leitmotto der Universität Leipzig:
Aus Tradition Grenzen überschreiten

- Grenzen: Humanities – Naturwissenschaften – Technik
- Tradition: Die philosophische Fakultät bis 1951

Was aber ist mit Technik?

1838 Gründung der Königlich-Sächsischen Baugewerkenschule zu Leipzig unter Albert Geutebrück

1875 Gründung der Städtischen Gewerbeschule zu Leipzig als historische Wurzel für die ingenieurwissenschaftliche Ausbildung im Maschinenbau und in der Elektrotechnik

> Erkenntnis, dass Gewerbetreibende neben einer allgemeinen höheren Bildung noch einer gründlichen Fachbildung bedurften.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Ingenieur-Ausbildung in Leipzig (Auswahl)

1909	Königlich-Sächsische Bauschule
1914	Fachschule für Bibliothekstechnik
1920	Sächsische Staatsbauschule
1922	Höhere Maschinenbauschule Leipzig
1949	Fachschule für Energie Markkleeberg
1954	Hochschule für Bauwesen Leipzig
1956	Ingenieurschule für Gastechnik Leipzig
1965	Ingenieurschule für Automatisierungstechnik
1970	Ingenieurschule für Energiewirtschaft Leipzig
1969	Ingenieurhochschule Leipzig
1977	Vereinigung zur Technischen Hochschule Leipzig
seit 1992	Hochschule für Technik, Wirtschaft und Kultur

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Technik und Bildung

- PIACC - http://www.gesis.org/piaac - ist in aller Munde
  - Die OECD untersuchte mit der Bildungsstudie PIAAC Kompetenzen von Erwachsenen im internationalen Vergleich: Die Deutschen schneiden mittelmäßig ab. (Wirtschaftswoche, 08.10.2013)
- Humanities und Technik in der Schulbildung

  Das *Realgymnasium* wurde Mitte des 19. Jahrhunderts im Staat Preußen eingeführt. Im Gegensatz zu humanistischen Gymnasien, welche mit Altgriechisch und Latein einen altphilologischen Schwerpunkt setzen, fokussierten sich Realgymnasien auf Realien und moderne Sprachen.

  Nach 1900 Weiterentwicklung zu *Oberrealschulen* und *Gymnasien.*

  1965 Umbenennung aller dieser Bildungseinrichtungen der BRD in „Gymnasium“. (Quelle: Wikipedia)
- Die polytechnische Oberschule der DDR

  Die Attributierung polytechnisch beschreibt die Idee des allgegenwärtigen polytechnischen Unterrichts und die daraus folgende Verbindung von geistig-schöpferischem Denken und praktisch-produktiver Arbeit sowie gesellschaftlich-nützlicher Tätigkeit als grundlegendes Charakteristikum der Schule. (Quelle: Wikipedia)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Was ist Technik?

1) Artefakte menschlicher Tätigkeit, als *Produkte technischen Handelns*, entweder einzelne Apparate und Maschinen oder umfassender das gesamte jeweils vorhandene System materieller Mittel zur Umgestaltung der Natur für Zwecke des menschlichen Daseins.

2) *Handlungsorientierter Ansatz…* knüpft an die griechische Vorstellung von *techne* als einem *Verfahrenswissen* an, das den Menschen bei der Herstellung von Dingen leitet … und dadurch ein die Natur im reproduktiven wie manipulativen Sinne beherrschendes *technisches Können* ermöglicht. (Quelle: H. Petzold, Philosophie-Wörterbuch)

Technik und Sprache

Beispiel: Sven-Åke Johansson – Konzert für 12 Traktoren

Bildquelle: Höfgen 1996 Foto: Bahr,

http://www.sven-akejohansson.com

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Zwei Zugänge

Der Mensch als Werkzeuge nutzendes Wesen – als „Tool using animal“

oder

Der Mensch als Werkzeuge herstellendes Wesen – als „Tool making animal“

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Hintergrund und Zielstellung

- Neues *interdisziplinäres* Angebot der Informatik im Wahlbereich der Geistes- und Sozialwissenschaften (Bachelor)
- **Hintergrund:** Techniken, insbesondere digitale Techniken, sind aus dem Berufsbild auch von Geistes- und Sozialwissenschaften nicht mehr wegzudenken. Im Zentrum des Angebots steht die *praktische* Vermittlung entsprechender Fertigkeiten.
- **Ziel:** „Learning by doing“ – Arbeit in interdisziplinären Teams an praktischen Fragestellungen
- **Kapazität:** 20 Studierende aus dem Wahlbereich, weitere Studierende der Informatik
- Zwei Module mit ähnlichem Aufbau
  - Winter: „Interdisziplinäre Aspekte des digitalen Wandels“
  - Sommer: „Kreativität und Technik“

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Organisatorisches

Im Zentrum stehen Seminar und Praktikum zu einem der angebotenen Themen

- gemeinsam mit Studierenden der Informatik
- Im P*raktikum* ist im Team von 5..8 Teilnehmern ein Projekt-thema eigenverantwortlich zu planen und umzusetzen.
- Im *Seminar* sind Vorträge zu konzeptionellen Fragen zu erarbeiten und zu halten.

Prüfungsleistung: mündliche Einzelprüfung (30 Min.) mit Schwerpunkt auf Themen der Vorlesung und des Praktikums.

- Zulassungsvoraussetzung: erfolgreich absolviertes Praktikum sowie Seminarvortrag

Mehr zur Vorlesung und zum ganzen Modul im BIS-OLAT-Portal https://olat.informatik.uni-leipzig.de im Kurs **W13.BIS.Wahl.**

Der **Zugang** erfolgt mit den Daten Ihres studserv-Accounts. Bitte schreiben Sie sich dort in die **Gruppe w13.bis.gs** ein.

Modulprogramm

- Vorlesung: dienstags 9:15-10:45, Hs 15
- Seminar: donnerstags 17:15-18:45, SG 3-14
- Praktikum: Termine sind mit Tutor und Gruppe zu vereinbaren, wöchentliches Gruppentreffen zum Abgleich der Arbeiten am Thema, Einsatz einer modifizierten Scrum-Methodik zur Steuerung der Projektarbeit

Modalitäten für die weitergehende Einteilung werden im Seminar am 17.10. abgestimmt.

Workload: 10 LP = 1/3 des Workloads eines Semesters

- 70% des Workloads entfällt auf die eigene Arbeit (210 h = durchschnittlich 14 h pro Woche in 15 Wochen)
- Ziel: Abschluss der Hauptarbeiten bis Ende Januar

Privatsphäre

„Wenn wir unsere Privatsphäre nicht schützen, werden wir sie verlieren.“

Eric Schmidt, promovierter Informatiker
und Aufsichtsratsvorsitzender von Google
am 30. Mai 2013 an der Universität Leipzig

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Begriffe, die in der Diskussion gesammelt wurden

Vertrauen
Teilen
Radius, öffentlich, Bekannte, Freunde = privat, intim
Grenzen definiert jeder anders
Grenzverletzung *soll* nicht passieren
Distanz ist Distanz zu Personen
Einverständnis, vertragliches Verhältnis
Distanz ist vom Thema abhängig
Privatsphäre = Menschenwürde

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Zum Begriff der Privatsphäre

These: Privatsphäre im heutigen Verständnis ist eine kulturelle Errungenschaft der bürgerlichen Gesellschaft

- Privatheit grenzt einen inneren von einem äußeren Raum (Zustandsraum) ab, ohne den die Begriffe *Umwelt*, *Handeln* in einer Umwelt, *kooperatives Handeln* und damit letztlich *Subjekt* nicht sinnvoll zu fassen sind.
- Privatheit ist ein Verhältnis, das sich in der Interaktion zwischen Subjekten herstellt und reproduziert.
- Die *Privatsphäre* als subjektbezogener Begriff konstituiert sich aus den interpersonalen Privatheitsverhältnissen des Subjekts.
- Die *Privatsphäre* ist damit selbst vielschichtig strukturiert. Nach der Intensität der interpersonalen Privatheitsverhältnisse lassen sich grob ein *Außenbereich*, ein *Mittelbereich* und ein *Innenbereich* unterscheiden.

Privatsphäre

- Gewisse Formen faktischer Privatheit (Bau, Nest, Fluchtdistanz, Reviere) gibt es auch im Tierreich. Die *Grenzen* solcher Privatheit stehen unter verstärkter Beobachtung und sind durch Gewaltandrohung oder -anwendung befestigt.
- Die rechtsförmige Verfasstheit der bürgerlichen Gesellschaft zusammen mit dem Gewaltmonopol des Staates reduzieren die Möglichkeiten der Konstituierung von Privatsphäre durch private Gewalt gegenüber vorbürgerlichen Gesellschaften.
- In (ordnungs)-rechtlich wenig regulierten Bereichen gewinnt die Regulation durch „private Gewalt“ (die sich in praktischen Handlungsvollzügen entwickelnde „normative Kraft des Faktischen“) sowie Gestaltung durch *vertragsrechtliche Regulation* an Bedeutung
- Privatheit in der bürgerlichen Gesellschaft als rechtfsförmiger Begriff ist mit der Weiterentwicklung des Rechts selbst weiterzuentwickeln.

Privatsphäre

- Der Begriff der Privatsphäre (als Unterscheidung von Innerem und Äußerem mit einer funktional bedeutsamen Grenze) ist charakterisiert auch *kooperative Subjekte*.
- Die Privatsphäre von *Individualsubjekten* steht als Teil der allgemeinen Persönlichkeitsrechte unter dem besonderen verfassungsrechtlichen Schutz der bürgerlichen Gesellschaft.

> Der Schutz der Privatsphäre ist im deutschen Grundgesetz aus dem allgemeinen Persönlichkeitsrecht abzuleiten. Das besondere Persönlichkeitsrecht dient dem Schutz eines abgeschirmten Bereichs persönlicher Entfaltung. Dem Menschen soll dadurch ein spezifischer Bereich verbleiben, in dem er sich frei und ungezwungen verhalten kann, ohne befürchten zu müssen, dass Dritte von seinem Verhalten Kenntnis erlangen oder ihn sogar beobachten bzw. abhören können. Durch die Unverletzlichkeit der Wohnung (Art. 13 GG) und durch das Post- und Fernmeldegeheimnis (Art. 10 GG) wird der Schutzbereich konkretisiert. (aus Wikipedia)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Privatsphäre und Internet

- Privatsphäre im Internet ist Teil der allgemeinen Privatsphäre und kann ohne Berücksichtigung dieser Einbindung nicht sinnvoll erklärt werden.
- Privatsphäre im Internet spielt heute vor allem im Außen- und Mittelbereich eine Rolle. Eine entsprechende Abstufung der Sicherheitsmaßnahmen gegen äußeren Durchgriff ist sinnvoll.
- Bei der Gestaltung der Privatsphäre im Internet sind Subjekte in hohem Maße auf technische Dienstleistungen und damit auf externe Strukturen angewiesen, deren *Vertrauenswürdigkeit* sie angemessen einschätzen müssen.
- Es ist zwischen privaten *Daten* (Zustand) und zur Ausführung gelangenden *Algorithmen* (Zustandsänderung) zu unterscheiden, die für die Privatsphäre relevant sind.

Privatsphäre

- Ordnungsrechtliche Regelungen der Privatsphäre im Internet existieren erst in Ansätzen, so dass *angemessenes praktisches Handeln* sowie *kooperative Gestaltung* auf vertragsrechtlicher Basis Hauptformen der Ausformung eines Begriffs „Privatsphäre im Internet“ sind.
- Ein *angemessenes* Verständnis der technischen Bedingtheiten, Möglichkeiten und Restriktionen des Internets ist für die qualifizierte Gestaltung der eigenen Privatsphäre im Internet unerlässlich.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Privatsphäre und (digitale) Identität

Begriff der *Privatheit* als sich in der Interaktion reproduzierendes intersubjektives Verhältnis setzt einen *Begriff des Ich*, einer eigenen *Identität* voraus.

- Digitale Identität, multiple digitale Identität und Rollen
  - Ist Identität teilbar?
- Abstrakte Identität, textuelle Repräsentation
  - Webseite, Login, Begriff der Session
- Authentifizierung
  - Passwort, andere Authentifizierungsformen
- Autorisierung
  - *Ich* als Subjekt und als Objekt von Autorisierung

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

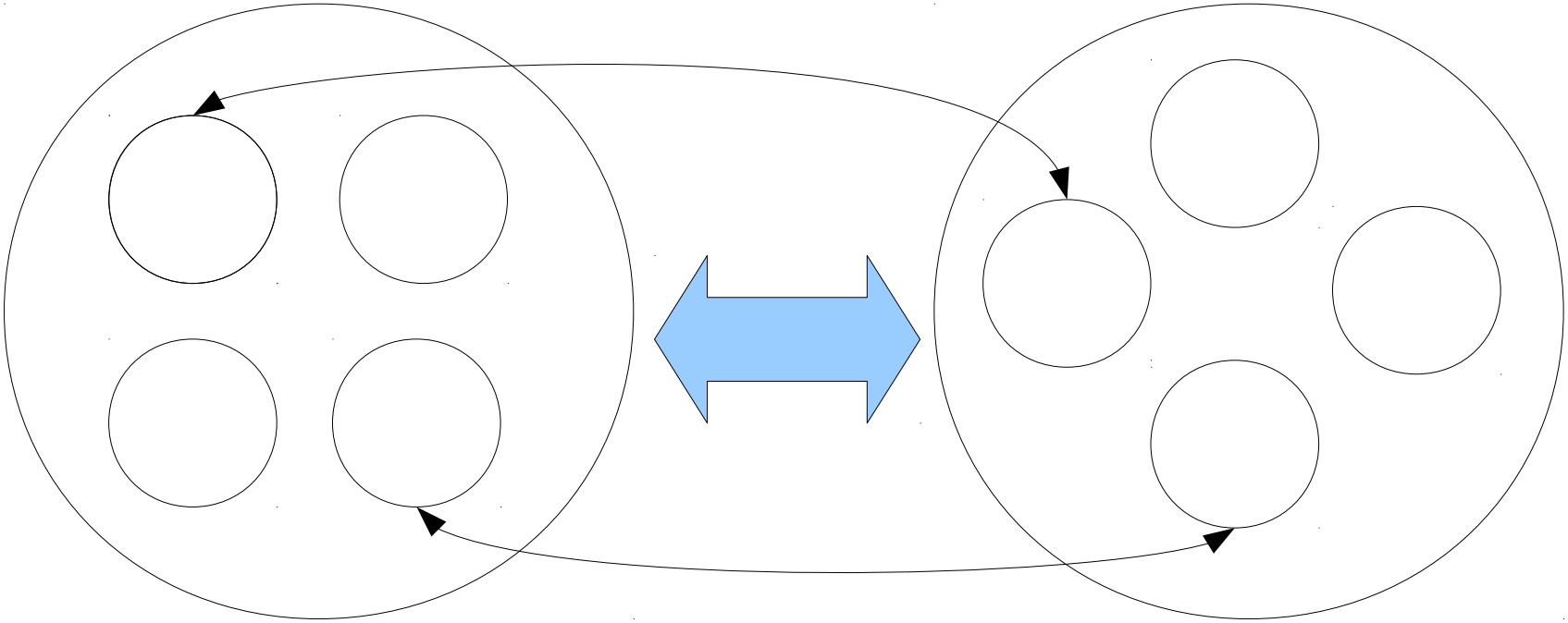
Der Rollenbegriff der Informatik

Ist Identität teilbar? Der Rollenbegriff der Informatik

- Als Rolle bezeichnet man in der Informatik ein Bündel von notwendigen *Erfahrungen, Kenntnisse und Fähigkeiten*, über die ein Mitarbeiter verfügen muss, um eine bestimmte *Aktivität* durchzuführen.
- Rollen sind dabei durch *Rollenbeschreibungen* innerhalb eines *Rollenmodells* definiert.
- Eine Rolle wird mit *Aktivitäten* und *Verantwortlichkeiten* verbunden.
- Für die Ausübung einer Rolle sind *Qualifikationsmerkmale* erforderlich.
- Eine Person kann mehrere Rollen inne haben. Mehrere Personen können jeweils die gleiche Rolle inne haben.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Rollen und Identitäten in der digitalen Kommunikation



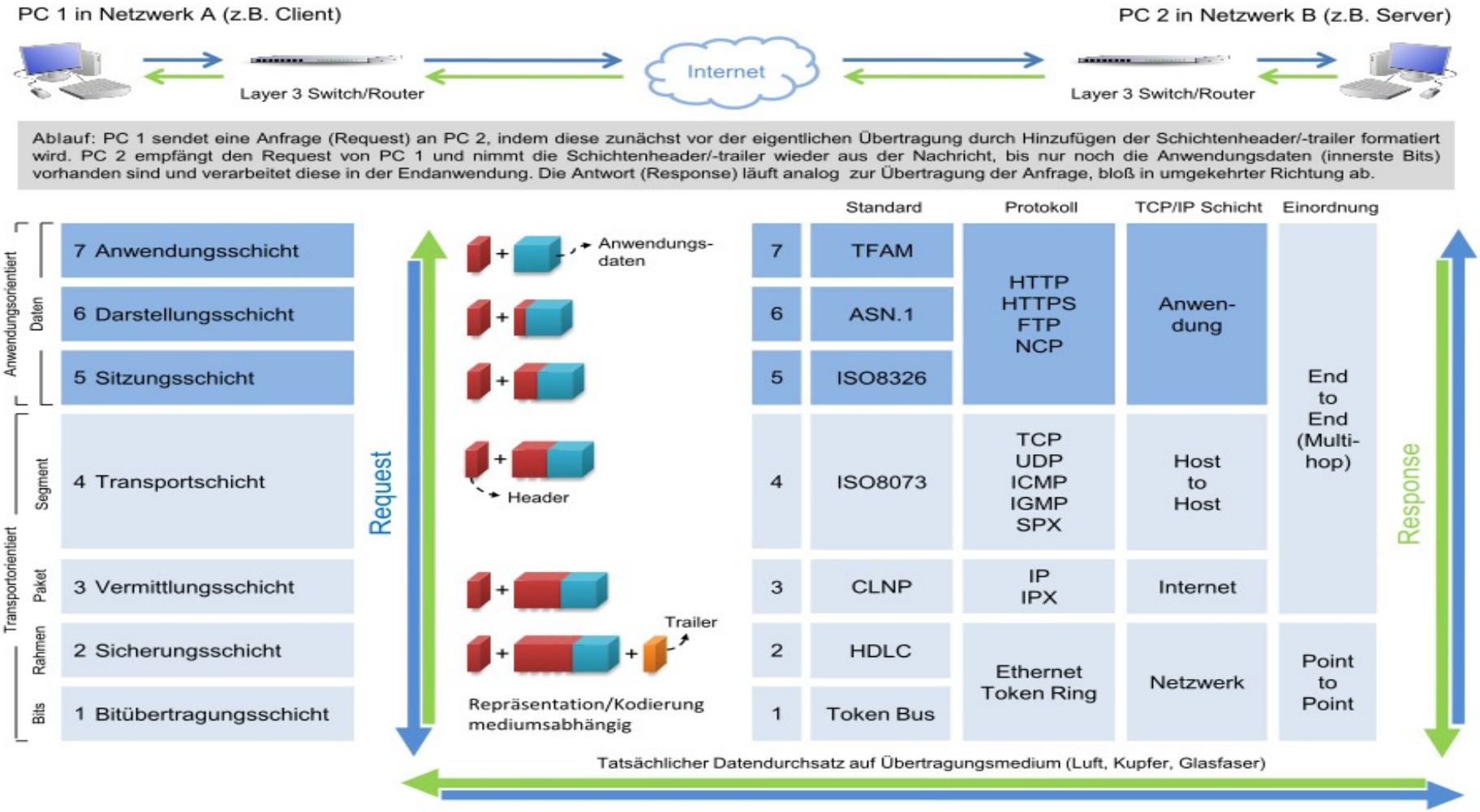
Internet Basics

Wir wollen im Weiteren den Begriff der *Rolle* als partielle Identität zu Grunde legen, wenn wir nun die technischen Gegebenheiten des Agierens digitaler Identitäten (genauer: *als* digitale Identitäten) betrachten wollen.

Zugang zum Internet, das OSI 7-Schichten-Modell

- http://de.wikipedia.org/wiki/OSI-Modell
- Schichten und Protokolle
- Protokolle und Sprache

Kommunikation im OSI-7-Schicht-Modell (Open Systems Interconnection Reference Model)



Quelle: Wikipedia, http://de.wikipedia.org/wiki/OSI-Modell

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie das Internet funktioniert

Texte bestehen aus Zeichen (Buchstaben, Zahlen usw.)

- Bits und Bytes
- Reduktion auf standardisierte Bitfolgen und damit Zahlen
- Erstes beständiges Alphabet: ASCII (7 Bit) = 0..127
  - 0..31 – Steuerzeichen
  - 32..127 – Zahlen und Buchstaben des englischen Alphabets
- Mehrere Standardisierungswellen für weitere Alphabete und Zeichensysteme (latin-1, Windows-Zeichensatz)
- Bedarf, sich zu einigen → Unicode
  - Beginn der Bemühungen um 1988
  - Erster Standard 1991 enthielt $2^{16} = 65.536$ Zeichen

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie das Internet funktioniert

Unicode

- Internationaler Standard, in dem langfristig für jedes Sinn tragende Schriftzeichen oder Textelement aller bekannten Schriftkulturen und Zeichensysteme ein digitaler Code festgelegt wird, um den Austausch textueller Information weltweit zu vereinheitlichen. Unicode wird ständig um Zeichen weiterer Schriftsysteme ergänzt.
- Hexadezimale Darstellung, etwa U+01FA (2 Byte)

UTF-8 als sich entwickelnder de-facto-Standard

- Kodierung von Zeichen in bis zu 4 Byte (variable Länge)
- Kodierung der ASCII-Zeichen in 1 Byte

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie das Internet funktioniert

Datenübertragung im Internet

- Serielle Übertragung als Bitfolge, für menschenlesbare Zwecke meist im Oktal- oder (häufiger) Hexadezimal-system (Basis 16) dargestellt (x1FA = 0001.1111.1010)
- Bitstrom wird in Pakete konstanter Länge zerteilt und mit Sender/Empfänger-Informationen (Routing) losgeschickt
- Pakete werden von Rechner zu Rechner weiter geleitet, bis sie ihren Empfänger erreicht haben
  - Integritätsprüfung mit einer Hash-Funktion
- Empfänger setzt aus den Paketen den Bitstrom wieder zusammen
- Damit dies für den Nutzer transparent ist, werden standardisierte Protokolle verwendet

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie das Internet funktioniert

Funktion	OSI Schichtenmodell	Protokolle (Auswahl)
Anwendungen	Anwendungsschicht Darstellungsschicht Sitzungsschicht	HTTP HTTPS SSH
Netzübertragung	Transportschicht Vermittlungsschicht	TCP/IP SSL/TLS
Netzzugang	Sicherungsschicht Übertragungsschicht	WLAN PPP Ethernet

Digitale Identitäten

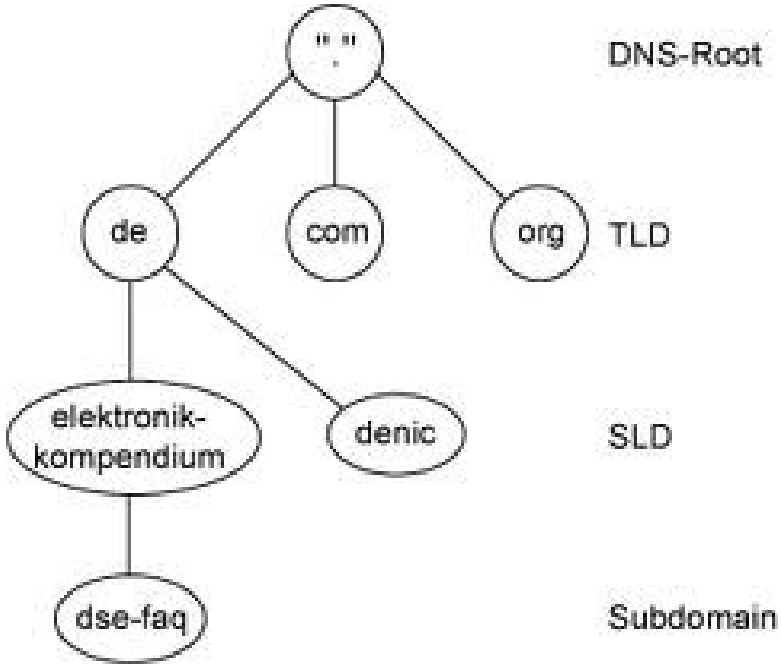
- Digitale Identität, Abstrakte Identität, textuelle Repräsentation
  - Webseite, Login
  - Begriff der Session (nicht nur auf Webseiten)
- Authentifizierung und Autorisierung

Wir werden im Weiteren unter einer *digitalen Identität* ein unter einer textuellen Repräsentation <name@rechnername> *authentifiziertes* und im Rahmen einer Session *autorisiertes* realweltliches Subjekt verstehen, das von dort aus Handlungen im digitalen Universum vornimmt.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Rechner und Rechnername

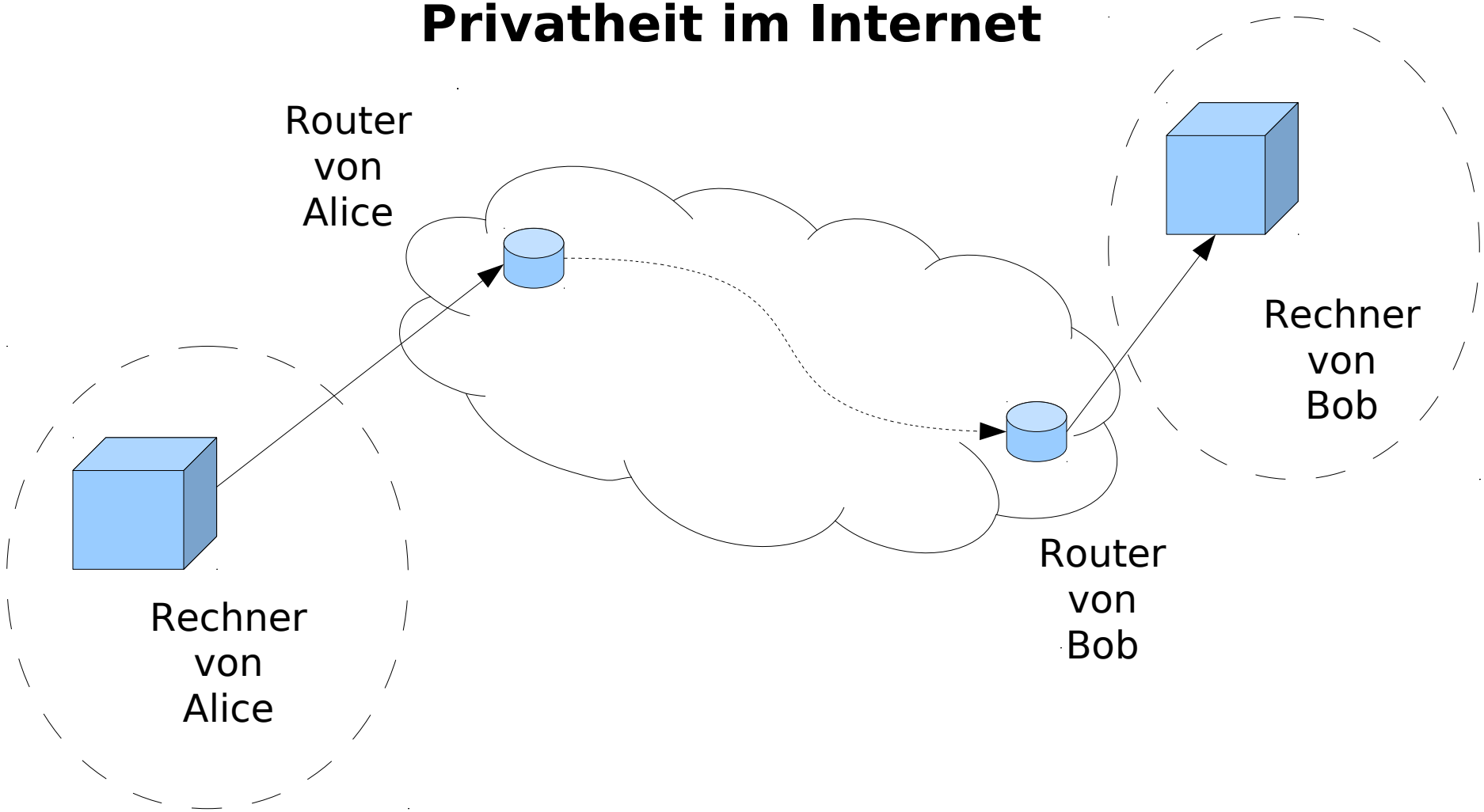
- Zum Aufbau von Rechnernamen, Domänennamen und Top Level Domänen
- Das ping-Kommando
- Umrechnung von Namen in Adressen – das Domain Name Service System



Quelle: http://www.imb-jena.de/~gmueller

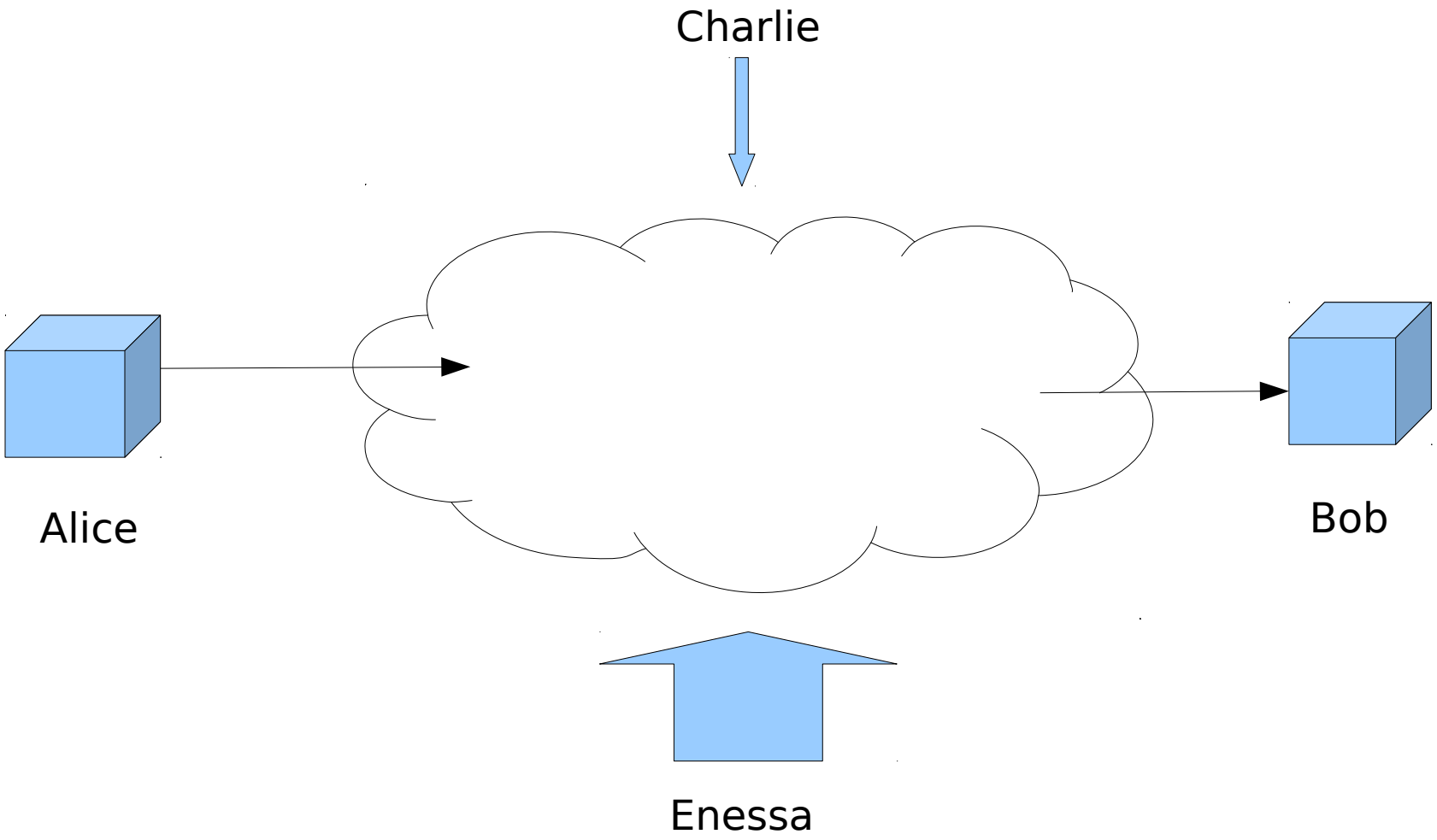
UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Privatheit im Internet



UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Privatheit im Internet



UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Was kann passieren?

- Mitlesen auf einem fremden Rechner
- Verhinderung der Nachrichtenzustellung
- Verfälschen von Nachrichten (Pakete modifizieren)
- Feststellen, mit wem kommuniziert wird, indem die Adressen der Pakete ausgelesen werden.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Vorfälle im Internet

Manipulationen der Paketzustellung

- Pakete nicht zustellen – Ägypten vom Netz
- Pakete gewisser Art nicht zustellen, Chinesische Mauer
- Anforderungen synchroner und asynchroner Kommunikation, Angebotskennungen, Priorisierung von Angeboten

Tracking – Paketverfolgung, Absender- und Senderkennungen

- ISP und Abrechnungsdaten
- ISP und Telekommunikationsgesetz
- Tor-Netzwerk, http://de.wikipedia.org/wiki/Tor_%28Netzwerk%29

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Vorfälle im Internet

Pakete an falscher Stelle zusammenführen

- Passiv: an drittem Ort, um mitzulesen
- Aktiv: Kommunikationspartner wird vorgespielt (Rechnerebene und Nutzerebene)

Einbruch in den Rechner

- Man kann nur einbrechen, wenn man eine digitale Identität hat
- Eigene Einbrecher-Identität: Bot-Netze, nur für Rechner interessant, die dauerhaft am Netz sind
- Nutzung vorhandener Identitäten: Admin-Account
- Nutzung Ihrer Identität

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Verschlüsselung im Internet – Basics

- Informationen werden als Pakete weitergegeben.
- Pakete sind Bit-Felder konstanter Länge, also letztlich *Zahlen.*
- Steganografie.
- Blockchiffre und Stromchiffre.
- Wir betrachten im Weiteren nur Blockchiffren.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Verschlüsselung im Internet – Basics

Erster Ansatz

- v: Z → Z und e: Z → Z als Ver- und Entschlüsselungs-funktionen auf Start- und Zielrechner (Prinzip der Punkt-zu-Punkt-Verschlüsselung)
- Geheimtext:=v(Klartext) wird übers Netz verschickt und beim Empfänger Nachricht=e(Geheimtext) erzeugt.
- Ansatz ist *Security by Obscurity*, denn v() und e() müssen *geheim* sein.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Verschlüsselung im Internet – Basics

Zweiter Ansatz

- Einbau eines textuellen Geheimnisses *(Schlüssel)* aus einem *Schlüsselraum S.*
- v: (Z,S) → Z und e: (Z,S) → Z als (öffentlich bekannte!) Ver- und Entschlüsselungsfunktionen
- Schlüssel VS zum Verschlüsseln und ES zum Entschlüsseln werden erzeugt.
- Geheimtext:=v(Klartext,VS) wird übers Netz verschickt und beim Empfänger Nachricht=e(Geheimtext,ES) erzeugt.
- Erfordert *Geheimnisaustausch*, denn die Schlüssel müssen erzeugt oder ausgetauscht werden.
- Beispiele: Cäsar-Methode, XOR-Verschlüsselung

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Verschlüsselung im Internet – Basics

- Effiziente und zuverlässige Methode, das bei genügender Länge der Schlüssel und Verwendung von Einmal-Schlüsseln auch so gut wie nicht zu knacken ist.
- Heute verwendet man meist symmetrische Verfahren (v=e, man muss das Verfahren dann nur einmal implementieren).
- Umfassende Schwachstellenanalyse der öffentlich bekannten (!) Verfahren e=v und Implementierungen (Open Source!) möglich.
- Problem: Sicherer Austausch der Schlüssel. Dazu werden heute die etwas teureren Public-Key-Verfahren verwendet.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Verschlüsselung im Internet – Basics

Public-Key-Verfahren

- Idee: Vom Schlüsselpaar VS und ES muss nur ES weiter gegeben werden. Wir verwenden ein *öffentlich bekanntes* Verfahren v(_,s) mit zusätzlichen Eigenschaften
- Jeder erzeugt sich ein Schlüsselpaar: Alice (ga, oa) und Bob (gb, ob) und *veröffentlichen* oa bzw. ob.
- Alice sendet Geheimtext an Bob:

  Geheimtext=v(Klartext, ob)
- Bob entschlüsselt

  Nachricht=v(Geheimtext,gb)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Verschlüsselung im Internet – Basics

- Aber kann sich Bob sicher sein, dass die Nachricht von Alice ist? Nein!
- Modifikation:

Geheimtext=v(v(Klartext,ga),ob)

Nachricht=v(v(Geheimtext,gb),oa)

- Damit das funktioniert, muss zusätzlich gelten

v(v(Text,g_),o_)=v(v(Text,o_),g_)=Text

- Bedingung erfüllt für Cäsarverschlüsselung (o=-g) und XOR-Verschlüsselung (o=g), aber: Wer o kennt, kann g leicht ausrechnen.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Grundlagen des Rechnens mit Resten

- $a \equiv b \pmod{m} \leftrightarrow a=b+x \cdot m$
- Rechnen mit Resten, prime Reste und Kürzungsregel
- Potenzreste mit http://wolframalpha.com
  Table[2^k mod 23,{k,1,50}]
- m und φ(m). Inverse Restklasse a^(-1) (mod m)
- Berechnung von φ(m) für primes m und für m=p·q
- Kosten modularer Arithmetik l-stelliger Zahlen
- Schnelles Potenzieren. Kosten O(l^3)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

RSA-Verschlüsselung

- http://de.wikipedia.org/wiki/RSA-Kryptosystem
- RSA ist ein von Rivest, Shamir und Adleman 1977 vorgeschlagenes asymmetrisches kryptographisches Verfahren auf der Basis der Annahme, dass das Faktorisieren großer Zahlen schwierig ist.
- Ansatz: $m=p \cdot q$, $\varphi(m)=(p-1) \cdot (q-1)$. Wähle zwei Zahlen v,e prim zu m als Exponenten und berechne

$$\text{Geheimtext} = \text{Klartext}^v \pmod m$$
$$\text{Nachricht} = \text{Geheimtext}^e \pmod m$$

- Notwendig: $(x^v)^e = x^{(v \cdot e)} = x \pmod m$, also

$$v \cdot e = 1 \pmod{\varphi(m)}$$

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

RSA-Verschlüsselung

- Es ist

$$(x^v)^e = (x^e)^v = x^{(v \cdot e)},$$

  die Zusatzbedingung also erfüllt.

- Öffentlicher Schlüssel ist (e, m), privater Schlüssel (v, m). Meist wird e=65537=2^16+1 genommen (die vierte Fermatsche Primzahl) und fest in das Verfahren eingebrannt, so dass nur m als öffentlicher Schlüssel bekannt gegeben werden muss.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Public-Key-Verschlüsselung: Allgemeines Prinzip

- Endliche multiplikative Struktur E mit 1 (Gruppe) und φ(E) Elementen. Dann ist a^φ(E) = 1 für alle a ∈ E.
  - Bei RSA ist $E=Z_m^*$, die Gruppe der primen Restklassen modulo m=p·q
- Wähle Exponenten v und e mit v·e = 1 (mod φ(E)). Dann ist (a^v)^e = (a^e)^v) = a
- Blockchiffre:
  - Interpretiere Blöcke als a ∈ E.
  - Geheimtext = Klartext^v
  - Entschlüsselter_Text = Geheimtext^e

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Anwendungen

- SSH - http://de.wikipedia.org/wiki/Secure_Shell
- Browserzertifikate: Firefox > Bearbeiten > Einstellungen > Erweitert > Zertifikate
- known_hosts, authorized_keys

Hashfunktionen

- h: K → S, Zuordnung einer Prüfzahl zu einer Datei, um deren Integrität zu sichern.
- http://de.wikipedia.org/wiki/Hashfunktion

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie sicher ist RSA?

- Siehe http://de.wikipedia.org/wiki/Secure_Shell zum Zusammenspiel von symmetrischer uns asymmetrischer Verschlüsselung
- Siehe http://de.wikipedia.org/wiki/RSA-Kryptosystem zu prinzipiellen Angriffsmöglichkeiten auf RSA

Wie sicher sind Hashfunktionen?

- Siehe Diskussion unter http://de.wikipedia.org/wiki/Secure_Hash_Algorithm

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Was bedeutet es, Technik zu vertrauen?

- Grundsicherheit, Fehlbarkeit, Erfahrungswerte
- Gewährleistung, Infrastruktur, Standards, Technik
- Kostet etwas
  - Soziologen: Alles ist eine Kosten-Nutzen-Rechnung, homo oeconomicus, rational choice (aber homo faber?)
  - Arbeitswerttheorie: Geld als Maß dessen, was man auf anderes Bedürfnis hin getan hat, um in gleichem Umfang eigenes Bedürfnis auf Kosten anderer zu befriedigen.
- Vertrauen und Erwartungen
  - Blindes Vertrauen, Wegschauen
  - *Können* wir überhaupt überall hinschauen?
  - Begründete Erwartungen

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Was bedeutet es, Technik zu vertrauen?

- Wie entwickeln sich die eigenen begründeten Erwartungen?
  - Entwicklungsaspekt, Rolle von Erfahrungen auf dem eigenen Handeln, Übertrag aus dem Gestern ins Heute
  - Rolle anderer, Rolle von Wissenschaft
  - Strukturelle Ähnlichkeiten zum Thema Struktur der Privatsphäre
  - Unbedingt erforderlich ist, dies auf einer *interpersonalen* Ebene zu beschreiben.
  - Welche Rolle spielt Wikipedia in diesen interpersonalen Begründungen?

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Was bedeutet es, Technik zu vertrauen?

Technik als Infrastruktur: Erwartungen, Grundsicherheit, Fehlbarkeit, *Verlässlichkeit*

- Gewährleistung von *Bedingtheiten des Handelns*, damit Technik als (eine) Voraussetzung unseres Handelns.

- Was hat es mit Bedingtheiten des Handelns auf sich?
  - Technische und nicht-technische Bedingtheiten, eine sinnvolle Unterscheidung?
  - Die Grenze ist fließend und eher die zwischen (in der Vergangenheit hergestellten) Bedingtheiten und (heutigem zeitkritischem) Handeln
- Welche Bilder von Menschen?
  - Werkzeuge nutzender Mensch vs. Werkzeuge herstellender Mensch?
  - Homo oeconomicus vs. Homo faber?

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf welchen Grundlagen muss ein Bild von den Menschen aufbauen, mit dem sich diese Fragen einfangen lassen?

> Die erste Voraussetzung aller Menschengeschichte ist ... die Existenz lebendiger menschlicher Individuen. Der erste zu konstatierende Tatbestand ist ... die körperliche Organisation dieser Individuen und ihr dadurch gegebenes Verhältnis zur übrigen Natur. ... Alle Geschichtsschreibung muß von diesen natürlichen Grundlagen und ihrer Modifikation im Lauf der Geschichte durch die Aktion der Menschen ausgehen.
>
> Man kann die Menschen durch das Bewußtsein, durch die Religion, durch was man sonst will, von den Tieren unterscheiden. Sie selbst fangen an, sich von den Tieren zu unterscheiden, *sobald sie anfangen, ihre Lebensmittel zu produzieren ...* Indem die Menschen ihre Lebensmittel produzieren, produzieren sie indirekt ihr materielles Leben selbst.

Karl Marx, Friedrich Engels: Die Deutsche Ideologie,
http://mlwerke.de/me/me03/me03_017.htm

Technik und Vertrauen

Technikverständnis als *Gewährleistung* von Bedingtheiten unseres Handelns ist das enge Technikverständnis (tool using animal).

Technikverständnis als *Herstellen* von Bedingtheiten unseres Handelns ist das weite Technikverständnis (tool making animal).

Wie umfassend ist dieses „Herstellen“ zu verstehen?

> Die Weise, in der die Menschen ihre Lebensmittel produzieren, hängt zunächst von der Beschaffenheit der vorgefundenen und zu reproduzierenden Lebensmittel selbst ab. Diese Weise der Produktion ist nicht bloß nach der Seite hin zu betrachten, daß sie die Reproduktion der physischen Existenz der Individuen ist. Sie ist vielmehr schon eine bestimmte *Art der Tätigkeit* dieser Individuen, eine bestimmte Art, ihr Leben zu äußern, eine bestimmte *Lebensweise* derselben. Wie die Individuen ihr Leben äußern, so sind sie. Was sie *sind*, fällt also zusammen mit ihrer Produktion, sowohl damit, *was sie produzieren*, als auch damit, *wie sie produzieren*. Was die Individuen also sind, das hängt ab von den materiellen Bedingungen ihrer Produktion. (Ebenda)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Vertrauen und Erwartungen

- Wir hatten festgestellt: Vertrauen ist eng an *begründete* Erwartungen gebunden.
  - Gibt es blindes Vertrauen? Im (zeitkritischen) Handlungsvollzug kann nicht lange palavert werden. Vertrauen ist selbst Bedingtheit für kooperative Handlungsvollzüge.
- Wodurch sind begründete Erwartungen charakterisiert?
  - Wissenschaftlichkeit, „sicheres Wissen“?
  - Kooperatives Handeln setzt Vertrauen und damit Bezug auf die Begründungen anderer voraus.
- Überschaubarkeit von Begründungen
  - Abgleich mit den Begründungen anderer, denen ich vertraue, eigene Erfahrungen
  - Wikipedia: Vertrauen in große Community, die Falsches schnell ändert

Zwei Zugänge

1) Artefakte menschlicher Tätigkeit, als *Produkte technischen Handelns*, entweder einzelne Apparate und Maschinen oder umfassender das gesamte jeweils vorhandene System materieller Mittel zur Umgestaltung der Natur für Zwecke des menschlichen Daseins.

2) *Handlungsorientierter Ansatz…* knüpft an die griechische Vorstellung von *techne* als einem *Verfahrenswissen* an, das den Menschen bei der Herstellung von Dingen leitet … und dadurch ein die Natur im reproduktiven wie manipulativen Sinne beherrschendes *technisches Können* ermöglicht. (Quelle: H. Petzold, Philosophie-Wörterbuch)

Was ist Technik?

Der Mensch als Werkzeuge *nutzendes* Wesen – als „Tool using animal“

oder

Der Mensch als Werkzeuge *herstellendes* Wesen – als „Tool making animal“

Was ist Technik?

Dies ist eine weltanschauliche Frage von grundsätzlicher Bedeutung

- Technikverständnis als *Gewährleistung* von Bedingtheiten unseres Handelns – enges Technikverständnis (tool using animal). Die Bedingtheiten selbst werden nicht thematisiert.
- Poppers „offene Welt“ rational agierender Einzelwesen, die nach Kriterien eines „rational choice“ ihre ökonomischen (homo oeconomicus) oder auch technischen (homo faber) Entscheidungen treffen.

oder

- Technikverständnis als *Herstellen* von Bedingtheiten unseres Handelns – weites Technikverständnis (tool making animal).

Was ist Technik?

Herstellen von Technik in diesem umfassenden Sinne lässt sich nicht sinnvoll vom *Herstellen unserer Lebensbedingungen insgesamt* trennen.

> Die Weise, in der die Menschen ihre Lebensmittel produzieren, hängt zunächst von der Beschaffenheit der vorgefundenen und zu reproduzierenden Lebensmittel selbst ab. Diese Weise der Produktion ist nicht bloß nach der Seite hin zu betrachten, daß sie die Reproduktion der physischen Existenz der Individuen ist. Sie ist vielmehr schon eine bestimmte *Art der Tätigkeit* dieser Individuen, eine bestimmte Art, ihr Leben zu äußern, eine bestimmte *Lebensweise* derselben.
>
> Wie die Individuen ihr Leben äußern, so sind sie. Was sie *sind*, fällt also zusammen mit ihrer Produktion, sowohl damit, *was sie produzieren*, als auch damit, *wie sie produzieren*. Was die Individuen also *sind*, das hängt ab von den mate-riellen Bedingungen ihrer Produktion. (MEW 3)

Wir landen damit bei einem *praxisphilosophisch* zu fundierenden Weltbild, in dem die *Produktion unserer Lebensbedingungen* in einem umfassenden Sinne im Zentrum steht und das somit um einen adäquat gefassten *Begriff von Arbeit als Zentralkategorie* zu entwickeln ist.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie stellen wir unsere Lebensbedingungen her?

Was sind unsere Lebensbedingungen?

> Die erste Voraussetzung aller Menschengeschichte ist … die Existenz lebendiger menschlicher Individuen. Der erste zu konstatierende Tatbestand ist … die körperliche Organisation dieser Individuen und ihr dadurch gegebenes Verhältnis zur übrigen Natur. … Alle Geschichtsschreibung muß von diesen natürlichen Grundlagen und ihrer Modifikation im Lauf der Geschichte durch die Aktion der Menschen ausgehen. (MEW 3)

- Umfassendes Verständnis eines Begriffs von *Natur* als die vorgefundenen Bedingungen sowie von *Produktion* als in diesem Kontext bedingtes Handeln.
- Begriff der Gesellschaftlichen Natur des Menschen
- Gestern – Heute – Morgen
- Das Gestern ist die Bedingtheit des Handelns im Heute.

Herstellen der Lebensbedingungen

- Gestern – Heute – Morgen
  - Gestern: Begründungen, Handlungsplanung, Entwicklung von *Handlungskompetenz*
  - Heute: Handlungsvollzug
    - Zeitkritisch! Handeln unter „unvollständigen Informationen“
    - Privates Entscheiden, Handeln, Verantworten
    - Dazu sind gesellschaftlich herzustellen: Überschaubarkeit, Vertrauen, Verlässlichkeit
  - Morgen: Die Welt unserer Erwartungen
- *Begründete Erwartungen* sind also die Brücke vom Gestern ins Morgen
- Die Vielfalt privater Erwartungen erscheint gesellschaftlich als Multioptionalität künftiger Entwicklung

Herstellen der Lebensbedingungen

- Morgen ist das Heute das Gestern
  - Lessons learned: Abgleich der Ergebnisse des Handlungs-vollzugs gegen die Erwartungen
    = (individuelle) Erfahrungen
  - *Erfahrungen* sind die Brücke vom Morgen ins Gestern
- Zwei zentrale Herausforderung an Sozialisierung:
  - Sozialisierung der Begründungszusammenhänge als gesellschaftliche Weiterentwicklung von Handlungs-*kompetenz*
  - Sozialisierung der Handlungs*vollzüge* als gesellschaftliche Weiterentwicklung realer Weltgestaltung
- Kultur und Ökonomie
- Was muss ein Begriff von Technik auf dem Hintergrund dieser Sozialisierungszusammenhänge leisten?

Technik und Kultur

- Technik (im umfassenden Verständnis) ist eine spezielle *Form* an der Nahtstelle zwischen beiden Sozialisierungs-prozessen der Herstellung von Überschaubarkeit, Vertrauen und Verlässlichkeit
- Technik ist Einheit von Handlungsvollzug und Begründung und kann deshalb nicht sinnvoll ohne Menschen gedacht werden. Überall, wo Technik ein scheinbares Eigenleben entwickelt, ist eine *Fetischisierung von Technik* mit im Spiel.
- Fetischisierung und Entfremdung

> Entfremdung bezeichnet einen individuellen oder gesellschaftlichen Zustand, in dem eine ursprünglich natürliche Beziehung (zwischen Menschen, Menschen und Arbeit, Menschen und dem Produkt ihrer Arbeit sowie von Menschen zu sich selbst) aufgehoben, verkehrt oder zerstört wird. ...
>
> „Entfremdung“ ist der gesellschaftlich vorangetriebene und unumkehrbare Prozess der Aneignung der **Natur** und ihrer materiellen und geistigen Umgestaltung zu **Kultur** samt den Institutionen, die fremdbestimmt wirken, sobald sie die Menschen beherrschen und sich ihren individuellen und kollektiven Wünschen entgegenstellen. (Quelle: Wikipedia)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Die Welt des Wissens und die Welt des Geldes

- Zwei Sozialisierungsanforderungen: Wir brauchen eine Infrastruktur der Begründungen und eine Infrastruktur realen arbeitsteiligen kooperativen Handelns
- Geld als Sozialisierungsmedium und Äquivalententausch?

  Die Menschen beziehen also ihre Arbeitsprodukte nicht aufeinander als Werte, weil diese Sachen ihnen als bloß sachliche Hüllen gleichartig menschlicher Arbeit gelten. Umgekehrt. Indem sie ihre verschieden-artigen Produkte einander im Austausch als Werte gleichsetzen, setzen sie ihre verschiedenen Arbeiten einander als menschliche Arbeit gleich. Sie wissen das nicht, aber sie tun es. Es steht daher dem Werte nicht auf der Stirn geschrieben, was er ist. Der Wert verwandelt vielmehr jedes Arbeitsprodukt in eine gesellschaftliche Hieroglyphe.

  Quelle: Karl Marx, Das Kapital, Band 1
  http://www.mlwerke.de/me/me23/me23_049.htm

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Die Welt des Wissens und die Welt des Geldes

- Grundlegende Funktionsprinzipien der Welt des Geldes (als sozialer Intermediator materiellen Lebens)
  - Verwaltet das Gestern im Heute
- Grundlegende Funktionsprinzipien der Welt des Wissens (als sozialer Intermediator von Begründungszusammenhängen)
  - Verwaltet das Morgen im Heute
- Grundlegende Charakteristika beider Sozialisierungsformen

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Charakteristika der Sozialisierung produktiver Arbeit

Produktive Arbeit im Kapitalismus wird als *zweckmäßige Tätigkeit* sozialisiert, die individuell vollbracht wird, aber erst im Nachgang „am Markt“ ihre Bewertung erfährt.

1. Mit dem Tausch auf dem Markt findet ein Eigentumsübergang statt. Jedes Produkt hat zu jedem Zeitpunkt **genau einen** Eigentümer.
2. Die Zweckvorstellungen werden nicht erst im Zeitpunkt des Tausches entwickelt, sondern müssen bereits **a priori**, vor Beginn der Produktion, vorhanden sein
3. Produkte entfalten ihre größte Bedürfnis befriedigende Wirkung, wenn sie für einen **vorab bedachten und bekannten** Zusammenhang hergestellt werden.

Produktion findet nicht voraussetzungslos statt, sondern setzt die Existenz einer **produktiven Infrastruktur** voraus.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Charakteristika der Sozialisierung von Kompetenz

- Kompetenz ist geronnene Erfahrung (Wissen)
- Erfahrung wird individuell gewonnen und muss sozialisiert werden, um handlungsmächtiger zu werden.
- *Wissen* ist sozialisierte Erfahrung.
- *Kompetenz* entsteht als individuelles Herunterbrechen dieser sozialisierten Erfahrungen, ist also individuell verfügbares Wissen.

Eigenschaften von Wissen:

1. Das getauschte Wissen besitzen danach beide, es **vermehrt sich.**
2. Der Nutzen von interessantem Wissen lässt sich nicht vorab planen, er ergibt sich erst **a posteriori.**
3. Interessantes Wissen entfaltet seine volle Wirkung erst in unerwarteten, **vorab nicht bedachten Zusammenhängen.**

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

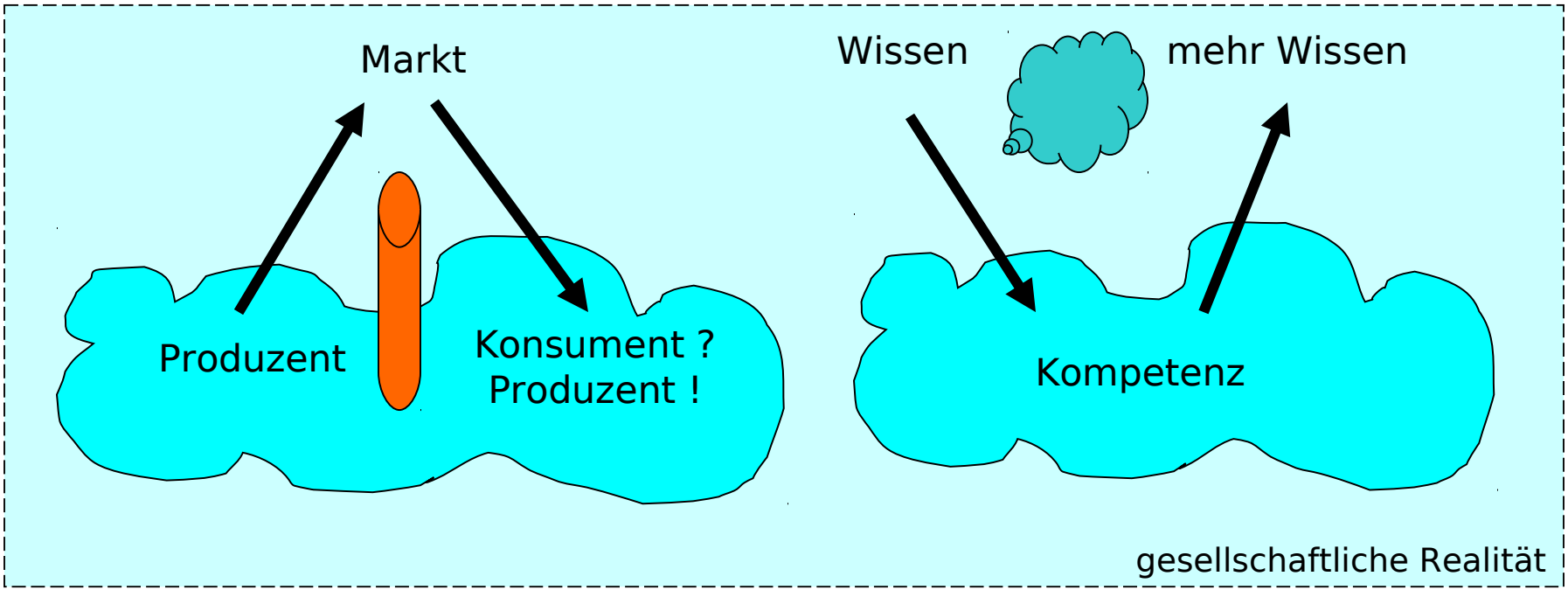
Vergleich

Die Sozialisierung produktiver Arbeit geschieht in der Form **gesellschaftlich vermittelter Individualität** – in der gesellschaftlich vermittelten Rückbezüglichkeit des "privaten Gebrauchs der Vernunft zum Handeln".

Die Sozialisierung von Kompetenz geschieht in der Form **individuell vermittelter Gesellschaftlichkeit** – in der individuell gebrochenen und in individueller Praxis neu aufgeladener Vorwärtsbezüglichkeit des "öffentlichen Gebrauchs der Vernunft zum Raisonnieren".

Gesellschaftlich konstituierte Erwartungen werden dabei durch institutionalisierte Handlungsvollzüge unter Einsatz von Technik(wissen) in Weiterentwicklung der Realität transformiert.

Parallelen zwischen Wissen und produktiver Arbeit



Produktive Arbeit ist
gesellschaftlich vermittelte Individualität

Wissen ist
individuell vermittelte Gesellschaftlichkeit

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Sozialisierungsmedien

- Sozialisierung von Handlungsvollzügen (Arbeit): Wie stellen wir unsere materiellen Lebensbedingungen her?
  - Bedingtheiten dieses Herstellungsprozesses – Geld und Eigentum.
  - Was ist Geld und die über Geld vermittelte Rationalität?
- Sozialisierung von Erfahrungen: Wie stellen wir unsere Begründungszusammenhänge her?
  - Bauen am „großen Puzzle“ der „einen großen Erzählung“
  - Bedingtheiten dieses Herstellungsprozesses
- Was passiert an den Nahtstellen beider Sozialisierungsformen?
  - Zum Begriff „geistiges Eigentum“

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wissenstechniken

- Handlungsvollzug ist zeitkritisch! Handeln unter „unvollständigen Informationen“
  - Privat gefordert: Entscheiden, Handeln, Verantworten
  - Gesellschaftlich dafür herzustellen: Überschaubarkeit, Verlässlichkeit, Vertrauen
- Wie produzieren wir Überschaubarkeit? Welche *Techniken* kommen zum Einsatz?
- Wie produzieren wir Verlässlichkeit? Welche *Techniken* kommen zum Einsatz?
- Wie produzieren wir Vertrauen? Welche *Techniken* kommen zum Einsatz?

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Zusammenfassung bisheriger Überlegungen

- Menschen *produzieren* ihre Lebensbedingungen
  - Sie produzieren *gesellschaftlich*
  - Herstellen eines *Vermittlungszusammenhangs* zwischen Gesellschaftlichem und Privatem
- So wie die Menschen *produzieren*, so *sind* sie
  - Basis eines Begriffs von *Kultur*
- Menschen produzieren ihre Lebensbedingungen durch *kooperatives Handeln*
- *Bedingtheiten* kooperativen Handelns
  - u.a. *Gebrauch* von Werkzeugen und Techniken
    - Mensch als „tool using animal“
  - Weiter Technikbegriff als *Verfahrenswissen*

Technik und Kultur

- Menschen *produzieren* auch die Bedingtheiten ihres Handelns
  - Mensch als „tool making animal“
  - Verschiedenheit der Semantiken von „tool“ in der englischen und „Werkzeug“ in der deutschen Literatur
- Gestern – Heute – Morgen
- Erfahrungen – Handlungsvollzüge – Erwartungen
  - Unterscheide auch hier individuelle und gesellsch. Ebene
- Zwei zentrale Herausforderung an Sozialisierung als Herstellung des Vermittlungszusammenhangs:
  - Sozialisierung der Handlungsvollzüge (A)
  - Sozialisierung der Begründungszusammenhänge (B)
- Menschen *produzieren* auch den Vermittlungszusammen-hang

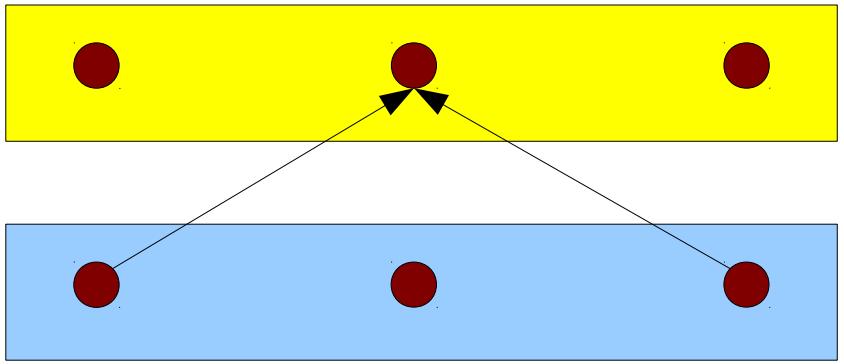
Übersichtlichkeit, Verlässlichkeit, Vertrauen, *Interessen*

Denken und Handeln

Erster Versuch, Zugang über zwei Sphären:

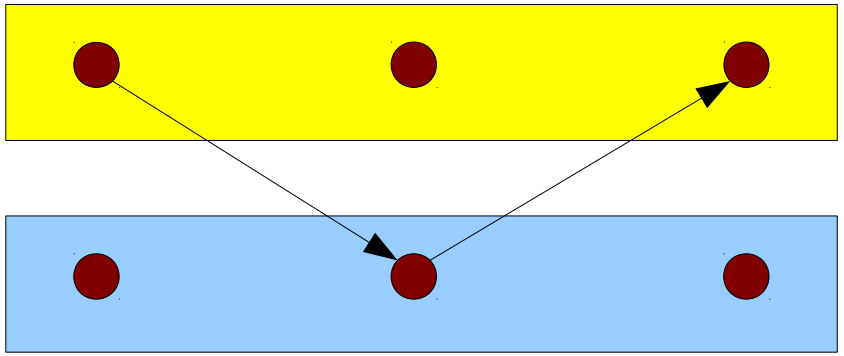
„Privater Gebrauch der Vernunft zum Handeln“

„Öffentlicher Gebrauch der Vernunft zum Raisonnieren“ (Kant)



Gestern – Heute – Morgen

Aber: 11. Feuerbach-these: „Die Philosophen haben die Welt nur ver-schieden interpretiert, es kömmt darauf an, sie zu verändern.“



UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Wie entsteht Zukunft? – Zusammenfassung

Gesellschaftlich konstituierte *Erwartungen* werden
auf der Basis *sozialisierter Erfahrungen*
durch *institutionalisierte Handlungsvollzüge*
unter Einsatz von *Technik(wissen)*
in Weiterentwicklung der Realität transformiert.

- Diskussion des Zugangs zweier synchron getakteter Parallelwelten auf dem Hintergrund einer Theorie des rationalen Handelns
  - Bewegt sich in der Linie der Tradition dualistischer Zugänge zur Welt, nach dem sich die Phänomene aus der kausalen Interaktion materielle und immaterieller Entitäten ergeben
  - Wesentliches Defizit: Die Welten des Denkens und des Handelns sind so eng miteinander verzahnt, dass ein Parallelwelten-Ansatz schnell ins Leere läuft.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Kultur, Technik, Sprache

„Technik gehorcht aufs Wort“. Wie mächtig ist Sprache? Welche Bedeutung hat Sprache bei der Produktion der Bedingtheiten unseres Handelns? Wie stehen die Begriffe *Sprache* und *Kultur* zueinander?

- „Er rührte an den Schlaf der Welt“
- Brecht: Fragen eines lesenden Arbeiters
- Daniel Everett: Language – the cultural tool

Technikeinsatz und deren Folgen

- Dual Use Problematik
- Grundsätzliche Ambivalenz von Technik

Erfordernis und Problematik des Herstellens einer gesellschaftlichen Übereinkunft über den Umgang mit spezifischen Technologien.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Kultur, Technik, Sprache

Das Herstellen einer solchen gesellschaftlichen Übereinkunft ist nur in einem *gesellschaftlichen Diskursprozess* um Ambivalenz von Technik möglich (Ergebnisebene – Erwartung).

- Dazu müssen solche Ambivalenzen *öffentlich* diskutiert werden. (Ebene des Handlungsvollzugs)
- Dazu müssen solche Ambivalenzen öffentlich *diskutierbar* sein. (Ebene der Bedingtheit von Handeln)
- Die Resultate dieser Diskussion müssen sich in den Begründungszusammenhängen unseres Handelns institutionalisieren (in Form von Sprache, als Kultur)

Dies ist ein wesentlicher Leistungsparameter der *Sozialisierung von Begründungszusammenhängen.*

- Aber: geistiges Eigentum, Betriebsgeheimnisse, ... als wesentliche Konfliktebene zur Sozialisierung von Handlungsvollzügen über Eigentum und Markt.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Petrinetz-Ansatz

- http://de.wikipedia.org/wiki/Petri-Netz
- Wesentliches theoretisches Konzept für das verteilte Rechnen (nebenläufige, kommunizierende Prozesse), vergleichbar in seiner Bedeutung mit dem der Turingmaschine für Einzelplatzrechner
- Entwickelt von Carl Adam Petri in dessen 1962 vorgelegten Dissertation (geb. am 26.1.1926 in Leipzig)
- Stellen und Transitionen = Denken und Handeln
  - Stellen = können Dinge lagern, speichern, darstellen, sich merken = passiv (Denken)
  - Transitionen = können Dinge erzeugen, verändern, vernichten = aktiv (Handeln)
- Petrinetze und Systeme mit verteiltem lokalem Speicher.
- Getaktete Petrinetze

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Technikentwicklung und Menschenbild

„Wie die Menschen produzieren, so sind sie“

- 1960er Jahre: In einer Welt mit neuen Möglichkeiten der Computer basierten Steuerung, Regelung und Simulation bekommt das Bild vom „rechnenden Menschen“ und „Mensch als Maschine“ neuen Auftrieb.
- Theoretische Grundlage: Konzept der Turingmaschine, eingeführt 1936 von Alan Turing.
- Kritik in Weizenbaums Buch „Macht der Computer und Ohnmacht der Vernunft“ (1976)
- Heute: In einer Welt des „Ubiquitous Computing“ bekommt das Bild vom Menschen als „kooperativem Agenten mit lokalem Speicher“ neuen Auftrieb.
- Theoretische Grundlage: Konzept des Petrinetzes bzw. neuronaler Netze
- Kritik formiert sich aktuell (Mittelstraß-Debatte)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Petrinetz-Ansatz und kooperatives Handeln

Problem auch dieses Ansatzes: Er fokussiert in seiner üblichen Ausprägung allein auf die Sozialisierung von Handlungsvollzügen, nicht aber auf die Sozialisierung von Begründungszusammenhängen.

- Dieses kann allein über den Abgleich der lokalen Speicher an den *Stellen* des Netzes erfolgen.
- Ein solcher Abgleich muss durch spezielle *Transitionen* vermittelt werden. Die Sozialisierung von Begründungszusammenhängen ist also ebenfalls nur über institutionalisierte Handlungsvollzüge (Sprachvollzüge) möglich.

Für *kooperatives* Handeln ist aber das *Herstellen* der Bedingungen als infrastrukturelle Leistung ebenfalls nur als *gemeinsames* Vorhaben denkbar.

- Geistiges Eigentum und kooperatives Handeln

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Voraussetzungen kooperativen Handelns

Für *kooperatives* Handeln ist das *Herstellen* der Bedingungen als infrastrukturelle Leistung ebenfalls nur als *gemeinsames* Vorhaben denkbar.

- Innen- und Außenverhältnisse kooperativen Handelns und die Diskussion um Privatsphäre
  - Betriebsgeheimnisse?
- Möglichkeiten der Gestaltung des Innenverhältnisses kooperativen Handelns, die Rolle von Sharing

Entwicklung einer Theorie der Freien Kooperation:

- Christoph Spehr: Die Aliens sind unter uns! Herrschaft und Befreiung im demokratischen Zeitalter. (1999)
  - Weltbild, Sprache und Kooperation. Zitat S. 45
- Christoph Spehr: Gleicher als Andere. Eine Grundlegung der Freien Kooperation. (2003)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Kooperatives Handeln und eine Kultur des Offenen

Christoph Spehr nimmt Debatten aus dem Kulturraum der amerikanischen Kultur-Linken auf, aus dem heraus wichtige *praktische* Entwicklungsanstöße in Richtung des Aufbaus einer Infrastruktur Freier Software kamen.

- Eben Moglen: Creators and Owners.
  - http://moglen.law.columbia.edu/publications/dcm.html
- Eigentum und Freiheit als die beiden Grundsäulen der bürgerlichen Ordnung.
  - Besondere Rolle von Software als *Prototyp* eines Produkts.
  - Sharing von Ideen und Traditionen akademischer Freiheit (im Sinne von Freizügigkeit)
- Kultur des Offenen (Free Culture)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

Vor-Gutenberg-Ära – Orale Kultur

- Weitergabe von Wissen vor allem mündlich, durch Erzählen auf verschiedenen Ebenen
- Wissen war damit etwas Fließendes, das aktuelle Erfahrungen aufnahm und entsprechend „fortgeschrieben“ wurde
- Entstehung eines „Common Sense“ – Rolle von Kirche und Religion, Ikonografie
- Bild von der Welt als „die eine große Story“ (der alte Siddhartha am Fluss)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

Erfindung des Buchdrucks

- Buch als *Werk*. Verschmelzen von Inhalt und Form.
- Haptische Wahrnehmung von Wissen als *Ding*.
- Neue Formen der Herstellung von „Common Sense“, in der die Buchdruckergilde eine herausgehobene Stellung einnimmt.
- 15. Jahrhundert: Copyright als Monopolrecht der Buchdruckergilde – Kopierrecht, gesichert durch die Krone
  - In beiderseitigem Interesse – ökonomische Interessen der Buchdrucker und Kontrolle der „öffentlichen Meinung“ durch die Herrschenden

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

„So, wie wir produzieren, so *sind* wir“

- Wahrnehmung von Ideen als dingliche Artefakte
  - Dinglichkeit und Zeitlosigkeit von Ideen (Kant)
  - Tradition der Reflexion über Wissen als „geniale Einzelleistung“
- Panta rhei – Wissen als prozessuales Element der Veränderung von Welt
  - Tradition der praktisch-ingenieurtechnischen Anwendung von Wissen
  - Newton: „Stehen auf den Schultern von Riesen“
  - Ideen als dauernde Rekombination. Fluss der Ideen als inhärent gesellschaftliche Leistung
  - Die Enzyklopädisten (insbesondere die Große Französische Enzyklopädie 1751–1765 unter Federführung von Diderot)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

Zwei Kulturen und zwei Säulen der bürgerlichen Rechtsordnung:

- Dinghafte Ebene des Seins → *Eigentum* als Basis von Verantwortungsfähigkeit
- Prozesshafte Ebene des Werdens → *Freiheit* (free as in free speech; Freizügigkeit) der Kombinierbarkeit

Verrechtlichung der bürgerlichen Gesellschaft im 19. Jahrhundert

- Verfassung der Vereinigten Staaten (Bill of Rights) vom 17. September 1787 als wichtiges Ergebnis des amerikanischen Unabhängigkeitskriegs
- Bürgerliches Gesetzbuch (1.1.1900) als erste Kodifikation im Privatrecht im Deutschen Reich.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

Die Anfänge können hier nicht umfassend dargestellt werden

- 1790: Copyright wird in der amerikanischen Verfassung verankert (regulär 14 Jahre Schutzfrist)
- Wesentliche Unterschiede zwischen anglo-amerikanischem und kontinental-europäischem Rechtsraum
- Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst
  - 1886 erste Fassung, 1908 Revidierte Berner Übereinkunft
  - Schutzdauer von mindestens 50 Jahren über den Tod des Urhebers hinaus
  - Harmonisierung der Schutzrechte, Gleichstellung von In- und Ausländern

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

Die geistigen Väter

- Deutliche Zunahme der wirtschaftlichen Bedeutung von Wissenschaft und Wissen im 20. Jahrhundert
- 50er Jahre: Fourastié sieht im Tertiären Sektor die bedeutendste Sphäre der Wertschöpfung der Zukunft
- 60er und 70er Jahre: Milton Friedman und die Chicagoer Schule – Theoretische Grundlegung für den Neoliberalismus
- Ende der 70er Jahre: Daniel Bell und die Postindustrielle Gesellschaft

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

Die Roadmap: Revidierte Berner Übereinkunft

- Weitere Versionen Rom 1928, Brüssel 1948, Stockholm 1967
- 1952 Welturheberrechtsabkommen UCC der UNESCO, um auch die USA mit ins Boot zu bekommen
- 1967 werden derartige Themen unter der Ägide der World Intellectual Property Organization WIPO zusammengefasst
- RBÜ, Pariser Fassung vom 24. Juli 1971 mit Präzisierung vom 29. Sept. 1979 – heute gültige Version
- 1973 – Beitritt der Sowjetunion zur RBÜ
- 1989 – Beitritt der USA zur RBÜ
- Heute 164 Staaten beigetreten

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

Die Roadmap: Die Befürworter formieren sich

- 1967 Gründung der WIPO als Dachorganisation zur weltweiten Verwaltung von Immaterialgüterrechte
- 1974 Aufwertung der WIPO zu einer Teilorganisation der UNO
  - Verwaltet heute RBÜ, Markenschutzabkommen, Harmonisierung des Patentwesens und des Umgangs mit gewerblichen Mustern und Modellen
- 1984 Gründung der International Intellectual Property Alliance IIPA zur weltweiten Durchsetzung des Konzepts „geistiges Eigentum“ als Rechtsbegriff
- 1986 Intellectual Property Committee IPC als die IIPA ergänzende Industrielobbyorganisation, um „geistiges Eigentum“ im Zuge der Uruguayrunde im GATT zu verankern

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

Die Roadmap: Die Befürworter formieren sich

- 80er Jahre – USA-Politik entwickelt verschiedene Strafmechanismen gegen Länder mit ungenügender IPR-Verrechtlichung
- 1995 TRIPS-1 – Trade Related Aspects of Intellectual Property Rights – als Teilergebnis der GATT-Verhandlungen, die zur Gründung der WTO führen
- 1996 WIPO Copyright Treaty – Mitgliedsstaaten müssen Rechtsschutz gegen Umgehung von Schutzmaßnahmen vorsehen
- 1998 DMCA – juristische Absicherung von Kopierschutzmaßnahmen in den USA
- 2001 – EU-Richtlinie zur Umsetzung der WIPO-Vorgaben in nationales Urheberrecht
- 2003 – UrhG-Novelle, Korb 1 in der BRD – „deutscher DMCA“

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Auf dem Weg zum „geistigen Eigentum“

- 2003 – UrhG-Novelle, Korb 1 in der BRD – „deutscher DMCA“
- Weitere deutsche Debatte: http://dini.de/ag/urhg/
- Themen:
  - § 31 a – Verträge über unbekannte Nutzungsarten
  - § 52 a – Öffentliche Zugänglichmachung für Unterricht und Forschung
  - § 52 b – Wiedergabe von Werken an elektronischen Leseplätzen in öffentlichen Bibliotheken
  - § 53 – Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch
- ACTA 2006 – 2012:
  - Mit Votum vom 4. Juli 2012 hat das EU-Parlament beschlossen, ACTA nicht zu ratifizieren, weshalb ACTA für die EU nicht in Kraft treten kann.
- TTIP seit 2012 … der nächste Versuch.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Die Wissenschaft setzt dagegen

Oktober 2003 – Berliner Erklärung über offenen Zugang zu wissenschaftlichem Wissen

- von namhaften europäischen und amerikanischen Forschungsorganisationen und Universitäten unterzeichnet
  - Bis März 2011 unterstützten mehr als 297 Institutionen aus der ganzen Welt die Forderung der Berliner Erklärung über offenen Zugang zu wissenschaftlichem Wissen.
- Unterzeichnende verpflichten sich, die Weiterentwicklung des Open-Access-Gedankens zu unterstützen, indem sie z.B. Forscherinnen und Forscher darin bestärken, ihre Ergebnisse im Open Access zu veröffentlichen
- Einbeziehung des kulturellen Erbes, also des in Archiven, Bibliotheken und Museen verwahrten Kulturguts, in die Forderung nach offenem Zugang

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Die Wissenschaft setzt dagegen

2004 – Göttinger Erklärung zum Urheberrecht für Bildung und Wissenschaft

- Gründung des *Aktionsbündnisses Urheberrecht* als Lobby-organisation der Wissenschaft im Kampf um die UrhG-Novellierung. http://www.urheberrechtsbuendnis.de
- Ende 2004 schließen sich auf der Basis der Göttinger Erklärung die sechs großen deutschen Wissenschaftsorganisationen Wissenschaftsrat, Hoschschulrektorenkonferenz, Max-Planck-Gesellschaft, Helmholtz-Gemeinschaft, Leibniz-Gemeinschaft, Fraunhofer-Gesellschaft und fast 200 weiteren Institutionen und 3.000 Einzelpersonen in diesem Bündnis zusammen
- Das Open Access Prinzip gewinnt damit im Wissenschafts-bereich zunehmend an Bedeutung, dem Prinzip förderliche Strukturen werden festgezurrt.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Die Wissenschaft setzt dagegen

2009 – Der Heidelberger Apell

Protest kommt aus den Reihen der Wissenschaft selbst, vorwiegend der Geisteswissenschaften. Die Unterzeichner sehen einen ungerechtfertigten Eingriff in die nach Art. 5 GG verbürgte Wissenschafts- und Kunstfreiheit.

Der Appell wird sehr kontrovers in der Akademia aufgenommen.

> Wenn man den Kampfbegriff der Enteignung schon in den Mund nimmt, dann sollte man ihn eher auf die bisherige Form des wissenschaftlichen Publizierens anwenden. Die lässt den Autoren zwar ihr Urheberrecht – das kann ihnen in unserem Rechtssystem ohnehin niemand nehmen –, aber alle Rechte der Verwertung seines geistigen Eigentums tritt der Autor an einen Verlag ab – und das meistens, ohne dass er am Erlös aus dem Verkauf seiner Texte beteiligt wird. Und just diese Knebelung soll dank Open Access gelockert werden. (Christoph Drösser in der ZEIT)

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Ein etwas weitere Perspektive

Die (Re)-Produktionsbedingungen Kreativer haben sich in den letzten 20 Jahren dramatisch verändert. Kreative haben in einer Welt restriktiver Besitztitel und immaterieller „Eigentums“rechte schlechte Karten und sind den Eignern und ihren Anwälten weitgehend schutzlos ausgeliefert.

> Zwei der Grundpfeiler der bürgerlichen Ordnung – bürgerliches Eigentum und bürgerliche Freiheit – treten damit in einen aktiven Widerspruch zueinander. (Eben Moglen, The dot Communist Manifesto, 2003)

Diese Probleme haben weitsichtige Kreative wie *Richard Stallman* schon in den frühen 80er Jahren eines erkennen lassen: Die nachhaltige Reproduktion der Schaffensbedingungen der Kreativen kann und darf den Eignern nicht überlassen werden.

Kultur des Offenen

Wenn der freizügige Zugriff auf die Kreationen anderer ein wesentlicher Teil dieser Schaffensbedingungen ist, dann *muss* dieser freie Zugriff auch gegen den Willen der Besitzenden durchgesetzt werden – selbst wenn die monetären Anreize immens sind: „Einmal kreativ sein und dann für immer Geld scheffeln“.

> „Free as in free speech not as in free beer“ ist eine Grundbedingung kreativen Schaffens, wird Richard Stallman nicht müde zu betonen.

Es liegt in der Hand der Kreativen selbst – denn sie sitzen ja an der Quelle –, die eigenen Schaffensbedingungen so zu organisieren, dass Wissen freizügig zugänglich ist und jede und jeder sich am gemeinsamen Wissen frei bedienen kann.

Kultur des Offenen

Mit dem *GNU-Projekt und Freier Software* hat dieser Gedanke zuerst in einem Bereich mit zentraler Bedeutung für die digitale Gesellschaft Fuß gefasst – dem Bereich, in dem die Werkzeuge der neuen Gesellschaft gebaut werden.

Mit der *GNU Public License* (GPL) wurde auch die Bedeutung einer adäquaten rechtlichen Regelung zeitig erkannt und erfolgreich „implementiert“.

Creative Commons dehnt diesen Ansatz auf andere Bereiche von Kultur und Kreativität aus, *Free Culture* (nach dem gleichnamigen Buch von Lawrence Lessig) erfasst die kulturelle Bedeutung eines solchen Prinzips.

Beide unterstützen die Fähigkeit der Kreativen, die eigenen Schaffensbedingungen nach eigenen Prinzipien zu gestalten.

Kultur des Offenen

Vom 13. bis zum 14. Dezember 2010 findet in Köln die internationale Expertenkonferenz „Open Access – Open Data“ statt. Sechs Jahre nach der ersten Open-Access-Konferenz in Köln gilt es, den Entwicklungsstand zu resümieren sowie die Herausforderungen für die nächsten zehn Jahre zu erörtern. Daneben sollen neue Wege für die immer bedeutender werdende Open-Data-Bewegung diskutiert werden.

Die Konferenz wird von Goportis organisiert. Goportis ist der Name des Leibniz-Bibliotheks-Verbundes Forschungsinformation, bestehend aus den drei deutschen zentralen Fachbibliotheken TIB (Technische Informationsbibliothek, Hannover), ZB MED (Deutsche Zentralbibliothek für Medizin, Köln/Bonn) und ZBW (Deutsche Zentralbibliothek für Wirtschaftswissenschaften – Leibniz-Informationszentrum Wirtschaft, Kiel/Hamburg).

Goportis ist in Deutschland zentraler Ansprechpartner für die Kompetenzfelder Volltextversorgung, Lizenzen, nichttextuelle Materialien, Langzeitarchivierung und Open Access.

Kultur des Offenen

Mit *Open Access* hat schließlich die Wissenschaftsgemeinde als Ganzes das Prinzip des freizügigen Zugangs zu den eigenen Produktionen zu einem ihrer zentralen Zukunftsprojekte erhoben, wie nicht zuletzt die Konferenz *Open Access and Open Data* noch einmal gezeigt hat.

Diesem Druck können sich mit den großen Wissenschafts-verlagen auch die bisherigen Verfechter restriktiver geistiger Eigentumsrechte kaum mehr entziehen – die ersten, wie etwa Springer sind längst umgeschwenkt und haben mit *Springer Open Access* Geschäftsmodelle aufgesetzt und etabliert, die den neuen Rahmenbedingungen Rechnung tragen.

UNIVERSITÄT LEIPZIG
Institut für Informatik
Betriebliche Informationssysteme

Kooperatives Handeln und eine Kultur des Offenen

- Eben Moglen: Creators and Owners.
  - http://moglen.law.columbia.edu/publications/dcm.html
- Eigentum und Freiheit als die beiden Grundsäulen der bürgerlichen Ordnung.
  - Besondere Rolle von Software als *Prototyp* eines Produkts.
  - Sharing von Ideen und Traditionen akademischer Freiheit (im Sinne von Freizügigkeit)
- Kultur des Offenen (Free Culture)