Didaktik der Sicherheit

Stefan Schumacher

Magdeburger Institut für Sicherheitsforschung

Chaos Computer Club Berlin
c-base
30.07.2011



Über Mich

- Direktor des Magdeburger Instituts für Sicherheitsforschung
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`
- Autoren/Fellows gesucht!



Über Mich

- `www.Kaishakunin.com`
  Sicherheitsberater mit langjähriger Beratungspraxis
  Social Engineering, Security Awareness,
  Organisationssicherheit
- B.A. Bildungswissenschaft und Psychologie;
  Schwerpunkte Personal- und Organisationsentwicklung,
  AO-Psychologie
- derzeit M.Sc.-Studium International Vocational Education
- Dieser Vortrag ist tagesaktuell aus meinem Forschungsprogramm



Über Mich

- `www.Kaishakunin.com`
  Sicherheitsberater mit langjähriger Beratungspraxis
  Social Engineering, Security Awareness,
  Organisationssicherheit
- B.A. Bildungswissenschaft und Psychologie;
  Schwerpunkte Personal- und Organisationsentwicklung,
  AO-Psychologie
- derzeit M.Sc.-Studium International Vocational Education
- Dieser Vortrag ist tagesaktuell aus meinem Forschungsprogramm



Inhaltsverzeichnis

1 Problem

2 Sicherheit messen und be-rechnen

3 Kompetenz

4 Resiliente Organisation



Warum das alles?

- Wer kann sich die Hände waschen?
- Wer kann sich die Hände desinfizieren?

Warum das alles?

- Wer kann sich die Hände waschen?
- Wer kann sich die Hände desinfizieren?
- Hygienische Händedesinfektion (min. 30 Sekunden) und Chirurgische Händedesinfektion (3-5 Minuten)



Warum das alles?

- Wer kann sich die Hände waschen?
- Wer kann sich die Hände desinfizieren?
- Hygienische Händedesinfektion (min. 30 Sekunden) und Chirurgische Händedesinfektion (3-5 Minuten)
- Ignaz Semmelweis, *Semmelweis-Reflex* bei *Paradigmenwechsel*

Warum das alles?

- Wer kann sich die Hände waschen?
- Wer kann sich die Hände desinfizieren?
- Hygienische Händedesinfektion (min. 30 Sekunden) und Chirurgische Händedesinfektion (3-5 Minuten)
- Ignaz Semmelweis, *Semmelweis-Reflex* bei *Paradigmenwechsel*

Warum das alles?

- IT breitet sich immer weiter aus
- IT-Sicherheit wird immer wichtiger
- Sicherheitsforschung tritt irgendwie auf der Stelle
- keine wirklichen Erfolge oder Fortschritte bezüglich IT-Sicherheit



Bsp: Buffer Overflow

- Zu große Daten werden in einen zu kleinen Buffer geschrieben
- Buffer-Grenzen laufen über, Speicher-Sicherheit wird verletzt
- Mögliche Konsequenz: Return-Adresse einer Sub-Routine wird mit beliebigen Daten überschrieben $\rightsquigarrow$ Root-Rechte
- Programmierer muss »nur« passende Befehle verwenden

...



Bsp: Buffer Overflow

- Zu große Daten werden in einen zu kleinen Buffer geschrieben
- Buffer-Grenzen laufen über, Speicher-Sicherheit wird verletzt
- Mögliche Konsequenz: Return-Adresse einer Sub-Routine wird mit beliebigen Daten überschrieben $\rightsquigarrow$ Root-Rechte
- Programmierer muss »nur« passende Befehle verwenden

...

Buffer Overflow in C

Das Problem

```
1 void input_line()
2 {    char line[1000];
3      if (gets(line))
4          parse_line(line);
5 }
```

`line` mit Länge 1000 deklariert
`gets` zeigt auf Array *ohne Länge*
wenn `line` größer 1000 = Problem
Thou shalt not follow the pointer



Buffer Overflow in C

Die Lösung

```
1 void input_line()
2 {    char line[1000];
3      if (fgets(line, sizeof(line), stdin))
4          parse_line(line);
5 }
```

`gets` zeigt auf Array *mit Länge*
Hardwarenahe Sprachen meiden, Compiler mit Feldüberwachung, PaX, `w^x` ...
Problem: Mensch muss entscheiden!



Eine kurze Geschichte des Buffer Overflows

- 02.11.1988: Morris-Wurm nutzte u. a. einen Buffer-Overflow via `gets()` in finger(1)
- 1996: Aleph One *Smashing the Stack for Fun and Profit* in Phrack 49
- 2001: Code Red
- 2008: SQL Slammer
- CORE-2007-0219: OpenBSD's IPv6 mbufs remote kernel buffer overflow
- 2007: Buffer Overflow in Snort
- VU#987308: HP LoadRunner buffer overflow vulnerability



Ariane 5 Flug 501

- 1996 Ariane 5 501: gesprengt nach 36,7 Sekunden
- Software von Ariane 4 auf Ariane 5 portiert
- 64 Bit Float in 16 Bit signed Int
- Beschleunigung der Ariane 5 ist signifikant höher $\rightsquigarrow$ Overflow
- Test-Simulation vor dem Flug fand das Problem nicht, Nicht-Schutz der Variablen war nicht dokumentiert
- 320 000 000,– € teures Feuerwerk
- maßgeblich verursacht durch Entscheidungen der Entwickler



Social Engineering

Jawoll, Herr Hauptmann ...



- Ausnutzen menschlicher Verhaltensweisen
- Warum soll ich versuchen einen Rechner zu cracken, wenn ich doch den Benutzer nur nach dem Passwort fragen muss?
- Profiling (aus Facebook & Co., Namen von Freunden, Lieblingsmusik, Urlaub in ...) $\rightsquigarrow$ Spear Phishing

Problemlage

- IT-Sicherheit wird *technisch* diskutiert
- und *technisch* gelöst
- Das reicht nicht!
- Menschen handeln und entscheiden!
- Diese Handlungen und Entscheidungen sind zu untersuchen und zu intervenieren
- Didaktik notwendig zur Professionalisierung
- Einführung eines neuen Sicherheitsbegriffs (Paradigmenwechsel)



Problemlage

- IT-Sicherheit wird *technisch* diskutiert
- und *technisch* gelöst
- Das reicht nicht!
- Menschen handeln und entscheiden!
- Diese Handlungen und Entscheidungen sind zu untersuchen und zu intervenieren
- Didaktik notwendig zur Professionalisierung
- Einführung eines neuen Sicherheitsbegriffs (Paradigmenwechsel)



Begriffe begreifen

- »mit dem Verstande erfassen«
- Begriff: Bedeutung bzw. Bedeutungsinhalt
- Syntax - Semantik - Pragmatik
- unterschiedliche Eigenschaften
- umgangssprachlicher Gebrauch
- Mächtigkeit: Mathematik, Datenbankentheorie, Unix-Programme, Geologie, Soziologie,
- Eigenschaften und Gebrauch müssen eingegrenzt werden Politik
- Definition *oder* Explikation



Definition

Definition

- sinnvolle Festlegung
- empirische Verankerung

VIVA-Kriterien in der Informatik
DIN EN ISO 12100 - Sicherheit von Maschinen für den Maschinenbau
DIN EN 61508 / VDE 0803: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer /programmierbarer elektronischer Systeme in der Elektrotechnik

Explikation

- Einführung präziser Begriffe für umgangssprachliche Begriffe
- *Explikandum*: unscharfer Begriff
- *Explikat*: scharfer Begriff
  - Ähnlichkeitsbedingung: Explikandum
  - Regelhaftigkeit: exakte Regeln
  - Fruchtbarkeit: möglichst viele genaue Aussagen
  - Einfachheit: Occams Razor



Informationssicherheit

Informationssicherheit wird in der Regel definiert über die VIVA-Kriterien

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität

menschliches Erleben und Verhalten wird ignoriert
Sicherheit einer Information kann so nicht beschrieben werden
Paradigmenwechsel nötig (vgl. Thomas S. Kuhn)

Informationssicherheit

Informationssicherheit wird in der Regel definiert über die VIVA-Kriterien

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität

menschliches Erleben und Verhalten wird ignoriert
Sicherheit einer Information kann so nicht beschrieben werden
Paradigmenwechsel nötig (vgl. Thomas S. Kuhn)



Was ist Sicherheit?

Meine Hypothese:

Sicherheit ist ein latentes soziales Konstrukt und muss als solches behandelt werden. Es werden neben technischen auch psychologische und soziologische Werkzeuge und Methoden benötigt. Soll die Sicherheit eines Systems verbessert werden, ist dazu eine Diagnose, Prognose und Intervention notwendig.



latentes soziales Konstrukt

- Konstrukt: nicht direkt messbarer Sachverhalt
- muss aus Indikatoren erschlossen/gemessen werden
- Messung der latenten (verborgenen) Variablen über manifeste (direkt zugängliche) Variablen
- Intelligenz: latentes Konstrukt, da nicht direkt messbar, Messung über Phrenologie (veralt.) oder Intelligenztests (ganz toll)
- Sicherheit kann nicht direkt gemessen werden
- Operationalisierung (Messbarmachung) durch manifeste Variablen notwendig



latentes soziales Konstrukt

- jedes Individuum *konstruiert* einen Sicherheitsbegriff
- wird dabei von der Gesellschaft beeinflusst
- beeinflusst die Gesellschaft (strukturelle Kopplung, Rekursion)
- Peter L. Berger, Thomas Luckmann *Die gesellschaftliche Konstruktion der Wirklichkeit*
- Bsp: Diskurse über Tschornobyl, Fukushima, Feinstaub, offene WLANs, Cyber-»War« usw.
- Wie mache ich diese Überlegungen für eine Didaktik fruchtbar?



latentes soziales Konstrukt

- jedes Individuum *konstruiert* einen Sicherheitsbegriff
- wird dabei von der Gesellschaft beeinflusst
- beeinflusst die Gesellschaft (strukturelle Kopplung, Rekursion)
- Peter L. Berger, Thomas Luckmann *Die gesellschaftliche Konstruktion der Wirklichkeit*
- Bsp: Diskurse über Tschornobyl, Fukushima, Feinstaub, offene WLANs, Cyber-»War« usw.
- Wie mache ich diese Überlegungen für eine Didaktik fruchtbar?



Inhaltsverzeichnis

1 Problem

2 Sicherheit messen und be-rechnen

3 Kompetenz

4 Resiliente Organisation



Sicherheit ist *normativ*

naturalistische Fehlschluss

- Die Aussage etwas ist sicher ist eine normative Aussage.
- Damit diese normative Aussage getroffen werden kann, ist eine Prämisse notwendig. Diese Prämisse heiße *Diagnosekriterium*.
- Ein Diagnosekriterium kann a priori oder a posteriori festgelegt werden.
- Die Menge aller Diagnosekriterien legt fest wie etwas zu sein hat, damit es als sicher bezeichnet werden kann.
- Die Anwendung der Diagnosekriterien auf eine Sache heiße *Sicherheitsdiagnose*.
- Die Anwendung der Sicherheitsdiagnose scheide Sachen in die Klassen sicher und unsicher



Sicherheit messen

oder: Wer ist zuständig?

- Wie kann Sicherheit gemessen werden?
- Wer definiert wie die Diagnosekriterien?
- Wer ist für einen Sicherheitsvorfall zuständig?
  Informatik, Software, Psychologie, Soziologie ...
- Welche Theorien, Werkzeuge und Methoden sind sinnvoll?
- Kann Sicherheit geschlossen (determiniert) werden?
- Berechnungsparadigma nach Heinz von Foerster

Sicherheit messen

oder: Wer ist zuständig?

- Wie kann Sicherheit gemessen werden?
- Wer definiert wie die Diagnosekriterien?
- Wer ist für einen Sicherheitsvorfall zuständig?
  Informatik, Software, Psychologie, Soziologie ...
- Welche Theorien, Werkzeuge und Methoden sind sinnvoll?
- Kann Sicherheit geschlossen (determiniert) werden?
- Berechnungsparadigma nach Heinz von Foerster

Berechenbarkeit der Sicherheit

oder: Wer ist zuständig?

triviale Maschine nach Heinz von Foerster

- alle möglichen Zustandsübergänge sind bekannt
- die Eintrittswahrscheinlichkeiten aller Zustandsübergänge sind bekannt
- Zustandsübergänge und deren Eintrittswahrscheinlichkeiten ändern sich mit der Zeit nicht, die Maschine ist daher:
- synthetisch determiniert
- analytisch determinierbar
- historisch unabhängig



Berechenbarkeit der Sicherheit

- Turing-Maschine == Algorithmus == Trivial-Maschine
- Computer-Programm == Trivial-Maschine
- Fehler in Computerprogrammen == triviales Problem
- theoretisch kann man die Fehlerfreiheit der Computerprogramme verifizieren
- bzw. nach Fehlern suchen lassen, sofern diese bekannt sind (Antivir, IDS etc.)

Donald E. Knuth

Beware Of Bugs In The Above Code; I Have Only Proved It Correct, Not Tried It.

Dimensionen der Sicherheit

Einteilung der Dimensionen anhand der Trivialität:

- technische Dimension: *Buffer Overflow im Code*
- psychische Dimension: *Warum hat der Programmierer den Buffer Overflow geschrieben?*
- soziale Dimension: *Wer hat wie geprüft ob der Code korrekt ist? Wer hat den Programmierer ausgewählt und weitergebildet?*



technische Dimension

- nur Fehler in Programmen
- Turing-Maschine $\rightsquigarrow$ deterministisch-determiniert
- technisches Problem $\rightsquigarrow$ technische Lösung
- Warum hat der Programmierer den Buffer Overflow eingebaut? $\rightsquigarrow$ soziale Dimension

technische Dimension

- nur Fehler in Programmen
- Turing-Maschine $\rightsquigarrow$ deterministisch-determiniert
- technisches Problem $\rightsquigarrow$ technische Lösung
- Warum hat der Programmierer den Buffer Overflow eingebaut? $\rightsquigarrow$ soziale Dimension

Soziale Dimensionen

Nach N. Luhmann

- psychische Dimension: intraindividuell
- soziale Dimension: interindividuell
- psychische D.: Arbeitspsychologie, Pädagogik
- soziale D.: Organisationspsychologie, Soziologie, Wissensmanagement, Organisationswandel



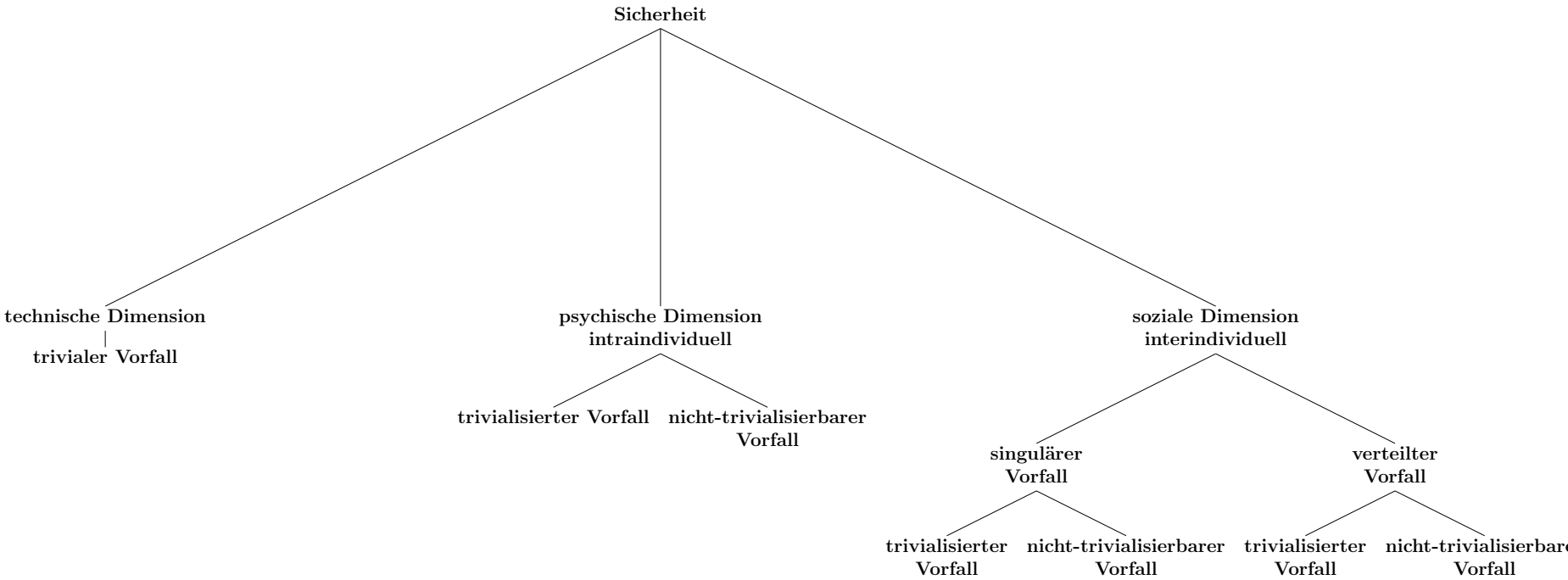
Soziale Dimensionen

Nach N. Luhmann

- psychische Dimension: intraindividuell
- soziale Dimension: interindividuell
- psychische D.: Arbeitspsychologie, Pädagogik
- soziale D.: Organisationspsychologie, Soziologie, Wissensmanagement, Organisationswandel

Taxonomie der Sicherheit

nach S. Schumacher



Anwendung in der Didaktik

- trivialisierte V.: Lösung bekannt, Lösung muss nur angewendet werden: Behaviorismus, Kognitivismus, Konstruktivismus
- nicht-trivialisierbarer V.: Lösung unbekannt, Individuum muss Lösung selbständig errechnen $\rightsquigarrow$ Handlungskompetenz, Ambiguitätstoleranz

Anwendung in der Didaktik

- trivialisierte V.: Lösung bekannt, Lösung muss nur angewendet werden: Behaviorismus, Kognitivismus, Konstruktivismus
- nicht-trivialisierbarer V.: Lösung unbekannt, Individuum muss Lösung selbständig errechnen $\rightsquigarrow$ Handlungskompetenz, Ambiguitätstoleranz
- Sicherheitskompetenz

Anwendung in der Didaktik

- trivialisierte V.: Lösung bekannt, Lösung muss nur angewendet werden: Behaviorismus, Kognitivismus, Konstruktivismus
- nicht-trivialisierbarer V.: Lösung unbekannt, Individuum muss Lösung selbständig errechnen $\rightsquigarrow$ Handlungskompetenz, Ambiguitätstoleranz
- Sicherheitskompetenz

Inhaltsverzeichnis

1 Problem

2 Sicherheit messen und be-rechnen

3 Kompetenz

4 Resiliente Organisation



Kompetenzen

Kompetenzmodell ist in der Berufspädagogik Gesetz: Handreichung für die Erarbeitung von Rahmenlehrplänen der Kultusministerkonferenz für den berufsbezogenen Unterricht in der Berufsschule und ihre Abstimmung mit Ausbildungsordnungen des Bundes für anerkannte Ausbildungsberufe



Kompetenzen

Definition

»Kompetenz befähigt einen Menschen zu selbstverantwortlichem Handeln und bezeichnet den tatsächlich erreichten Lernerfolg. Qualifikation ermöglicht die Verwertung von Kenntnissen, Fertigkeiten und Fähigkeiten«.

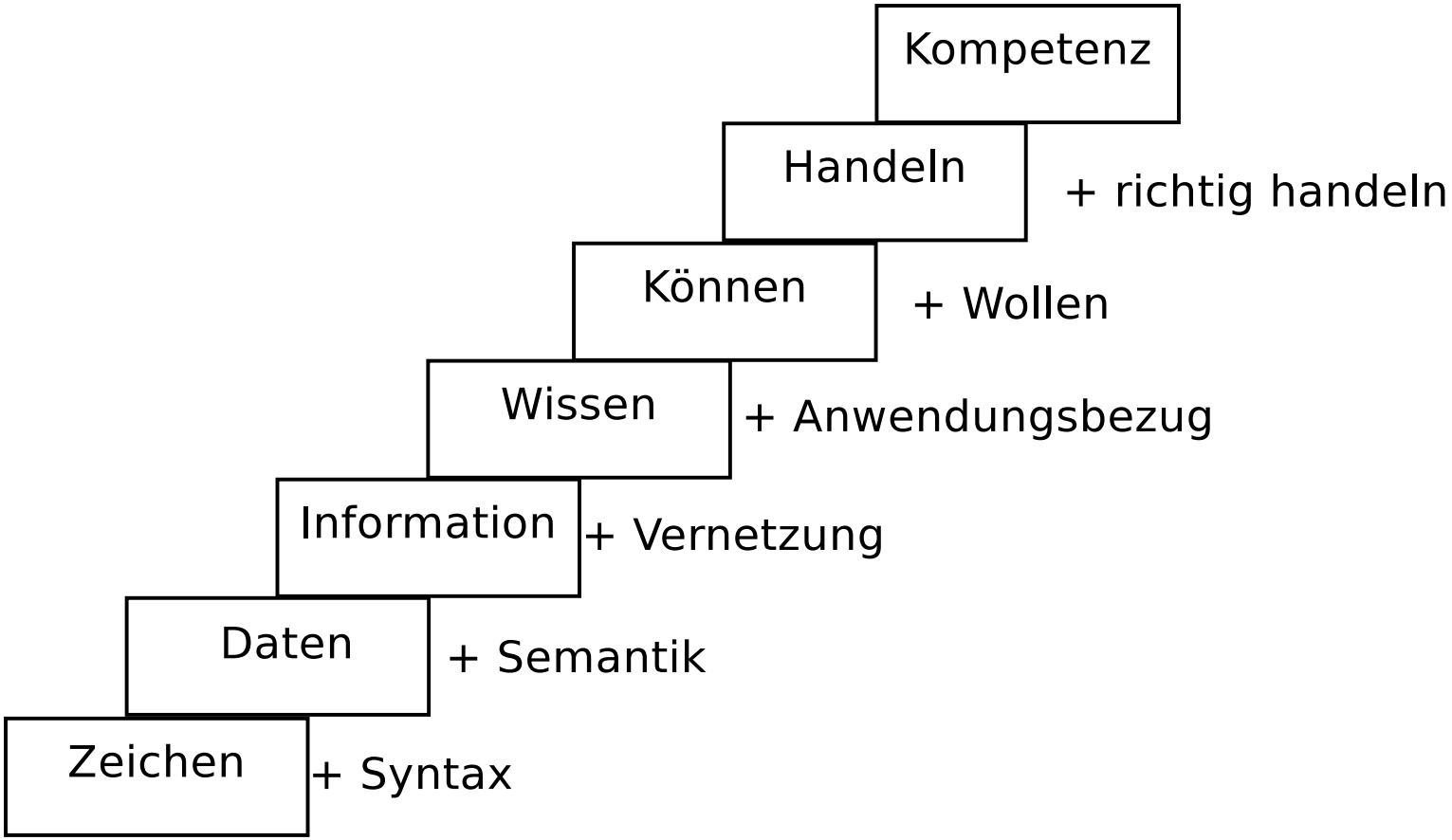
Michael Gessler: Das Kompetenzmodell *in* Handbuch Personalentwicklung – Die Praxis der Personalbildung, Personalförderung und Arbeitsstrukturierung, Schaeffer-Pöschel

Kompetenzen

Das Kompetenzmodell ist zur Zeit *das* Modell um Handlungen pädagogisch zu beeinflussen.
U.a. Umstellung aller Ausbildungsberufe auf Kompetenzmodelle
Kompetenzen in der Pisa-Studie

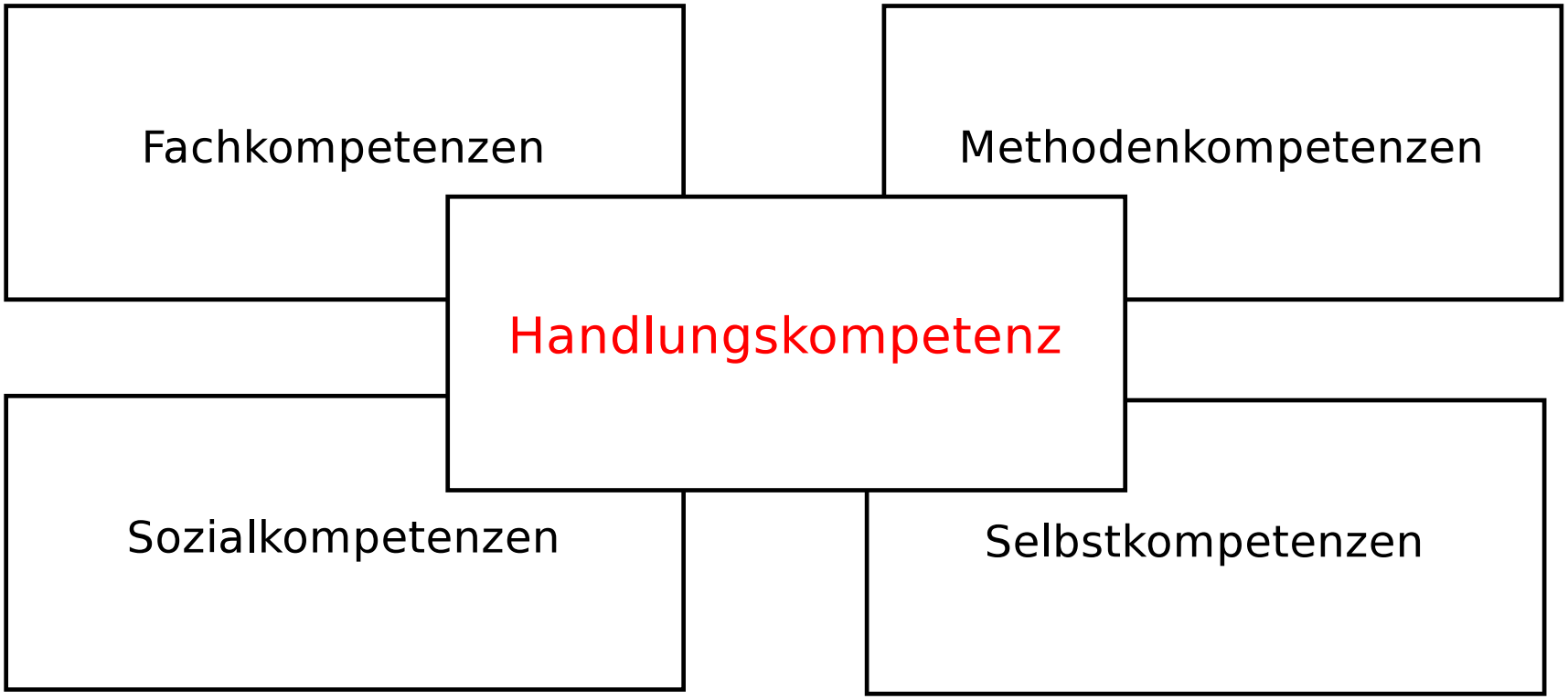


Wissenstreppe nach K. North (gekürzt)



Kompetenzmodell

- es gibt viele Definitionen/Explikation des Kompetenzbegriffs in der Personalentwicklung
- daher auch viele organisationsabhängige Kompetenzmodelle
- Kompetenzmodell steuert Kompetenzauswahl, Kompetenzevaluation und Kompetenzentwicklung
- organisationsabhängig, aber unabhängige Anteile (es gibt nicht das eine$^{[TM]}$ Kompetenzmodell)
- Kompetenzen grob gerastert (nach Erpenbeck/Rosenstiel)
  - Fachkompetenz
  - Methodenkompetenz
  - Sozialkompetenz
  - Persönlichkeitskompetenz
- führen in ihrer Anwendung zu Handlungskompetenz



Zusammenhang zwischen Kompetenzen (U.P. Kanning: Förderung sozialer Kompetenzen in der Personalentwicklung)

Fachkompetenz

Fähigkeit, berufstypische Aufgaben und Sachverhalte den theoretischen Anforderungen gemäß selbständig und eigenverantwortlich zu bewältigen

- Fachsprache, Fachmethoden und -verfahren und deren Anwendung, Sachkunde, Risiken- und Gefahren
- Bsp: *Zertifikat, digitale Signatur, MD5, CA-Cert, SSL, Man-in-the-Middle*



Methodenkompetenz

- Fähigkeit zur Anwendung bestimmter Lern- und Arbeitsmethoden, insbesondere zur selbständigen Erschließung unterschiedlicher Lern- und Wirklichkeitsbereiche
- Problemlösungstechniken, Entscheidungsfindungstechniken
- Lösungstrategien für neue Situationen (Transferleistung)
- Bsp: *Auswahl und Installation eines neuen Betriebssystems*



Sozialkompetenz

- Fähigkeiten, im sozialen Umfeld zu agieren
- zielorientiertes Handeln in sozialen Interaktionssituationen

Persönlichkeitskompetenz

- Methodenkompetenz (Selbstreflexion, Kreativitätstechniken)
- Lernkompetenz (individuelle Lerntechniken und -strategien, Lernumgebung gestalten)
- kommunikative Kompetenz (überreden/überzeugen, erklären/suggerieren)



Was ist noch zu tun?

- Fachkompetenzen müssen festgelegt werden
- Kryptographie, Session-Hijacking, Spoofing, ...
- Vermittlung dieser Fachkompetenzen (Fachdidaktik?)

Inhaltsverzeichnis

1 Problem

2 Sicherheit messen und be-rechnen

3 Kompetenz

4 Resiliente Organisation



Social Engineering

- Social Engineering auf Organisationsebene
- *verteilter Sicherheitsvorfall*
- Angriff gegen Alice, Bob, Charly und David
- jeder einzelne kann den Angriff nicht erkennen, da er nur ein Teil ist
- Erkennung auf organisationaler Ebene



Organisationssicherheit/Resiliente Organisation

Organisationssicherheit

Organisationssicherheit bezeichnet die Sicherheit einer Organisation auf technischer, sozialer und technisch-sozialer Ebene. Organisationssicherheit umfasst damit alle Dimensionen der Sicherheit.

Resiliente Organisation

Eine Organisation ist resilient, wenn sie auch bisher unbekannte Angriffe *erkennt* und auf diese reagieren kann. Eine Resiliente Organisation ist zwingend fähig zur Erkenntnis und zu kompetenten Handeln.



Kommunikation in Organisationen

- Wissensmanagement
- Lern- und Wissensbarrieren
- Lehr- und Lernkultur
- Organisation als System
- Awareness
- Organisation verhindert kompetentes Handeln oder ermöglicht es

Sicherheitskompetentes Handeln

- konstruktivistischer Ansatz
- Sicherheit als Teil der Weltanschauung
- Individuum konstruiert Sicherheit als Teil der Weltwahrnehmung
- Wie kann man die Weltwahrnehmung ändern?

Literatur

- Stefan Schumacher *Sicherheit messen. Eine Operationalisierun als latentes soziales Konstrukt* In: Die sicherheitspolitische Streitkultur in der Bundesrepublik Deutschland (2011)
- Jörg Sambleben & Stefan Schumacher (Hrsg): *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?*
- Stefan Schumacher: *Auf dem Weg zum Intrusion Detection System der nächsten Generation* in: Tagungsband Chemnitzer Linux-Tage 2010
- Stefan Schumacher: *Psychologische Grundlagen des Social-Engineering* Datenschleuder 94

