Vertrauen ist gut, Kontrolle unmöglich?

– Keynote –

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

Austrian Trust Circle
06.05.2015



Über Mich



Über Mich

- Studium Bildungswissenschaft/Psychologie
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Geek, Nerd, Hacker seit knapp 20 Jahren
- Mitarbeit im NetBSD und PostgreSQL Projekt
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- www.Sicherheitsforschung-Magdeburg.de



Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
- Lehrerfortbildung
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe
- IT-Sicherheit in KMU
  - empirische Grundlagenforschung
  - didaktische Aufbereitung
  - Schulungen



Schulungs- und Beratungsangebote

- Sicher unterwegs im Internet
- Anonymität und Überwachung im Internet
- Security Awareness Kampagnen konzipieren
- Netzwerke absichern/Penetration Testing
- Die psychologischen Grundlagen des Social Engineerings
- Der digitale Untergrund: zur aktuellen Bedrohungslage im Internet
- Kryptographie - Konzepte, Methoden und Anwendungen
- Strategien im Wirtschaftskrieg
- Selbstschutz in Krisengebieten



Inhaltsverzeichnis

1 Vertrauen?

2 Komplexität

3 Sicherheit?

4 Schwachstelle Mensch?

5 Didaktik



Vertrauen?

- Reflections on Trusting Trust
- Vertrauen ist gut, Kontrolle ist besser? Oder unmöglich?
- Was ist Vertrauen?
- Was Komplexität?
- Was ist Sicherheit überhaupt?
- Wie kann ich Sicherheit messen?
- Wie Sicherheit generieren?
- Psychologie der Sicherheit



Vertrauen

Ist Kontrolle möglich?

- Reflections on Trusting Trust
- 1984, Turing Award Speech, basiert auf
- Karger, Paul A.; Schell, Roger R. (June 1974). Multics Security Evaluation: Vulnerability Analysis
- Compiler wird manipuliert
- baut Backdoor in kompilierten Code ein
- Compiler kompiliert Backdoor in kompilierten Compiler ein ...



Vertrauen

Ist Kontrolle möglich?

- Verifikation technischer Systeme theoretisch möglich
- IT-Systeme sind zu komplex um wirklich überprüft zu werden
- NetBSD:ca. 163 000 Quelldateien, 57 228 442 LoC, 1 991 091 842 Zeichen
- Faust I: 4 600 Zeilen, 200 000 Zeichen
- der Verteidiger muss *alle* Systeme erfolgreich verteidigen, der Angreifer nur *eine einzige* Sicherheitslücke ausnutzen



Vertrauen

Ist Kontrolle möglich?

Ist GnuPG sicher?

1. GnuPG-Implementierung?
2. mutt?
3. vim?
4. Userland?
5. OS-Kernel?
6. Treiber-Blobs?
7. BIOS/UEFI?
8. Festplatte?
9. AES? SHA1?
10. Mathematik?
11. Gödel?



Vertrauen

laut Luhmann

- ein Mittel zur Reduktion sozialer Komplexität
- muss *immer* gewährt werden
- komplexere Umwelt erzwingt funktional ausdifferenzierte Systeme
- z.B. Medizin, Recht, Politik, Medien, Hacker, IT-Experten ...



Vertrauen

laut Luhmann

- Subsysteme müssen miteinander kommunizieren, Schnittstellen entstehen
- jeder Experte kann nicht alles wissen, da nicht die gesamte Umwelt aufgenommen werden kann
- d.h. Experten müssen zusammen arbeiten und einander vertrauen
- dazu haben sich Diagnosekriterien entwickelt
  z.B. formale Bildungsabschlüsse in D, Empfehlungsschreiben in USA, Familienbeziehungen in Saudi-Arabien
- Komplexität wird damit reduziert, Vertrauen gewährt



Inhaltsverzeichnis

1 Vertrauen?

2 Komplexität

3 Sicherheit?

4 Schwachstelle Mensch?

5 Didaktik



Komplexität

Informatik

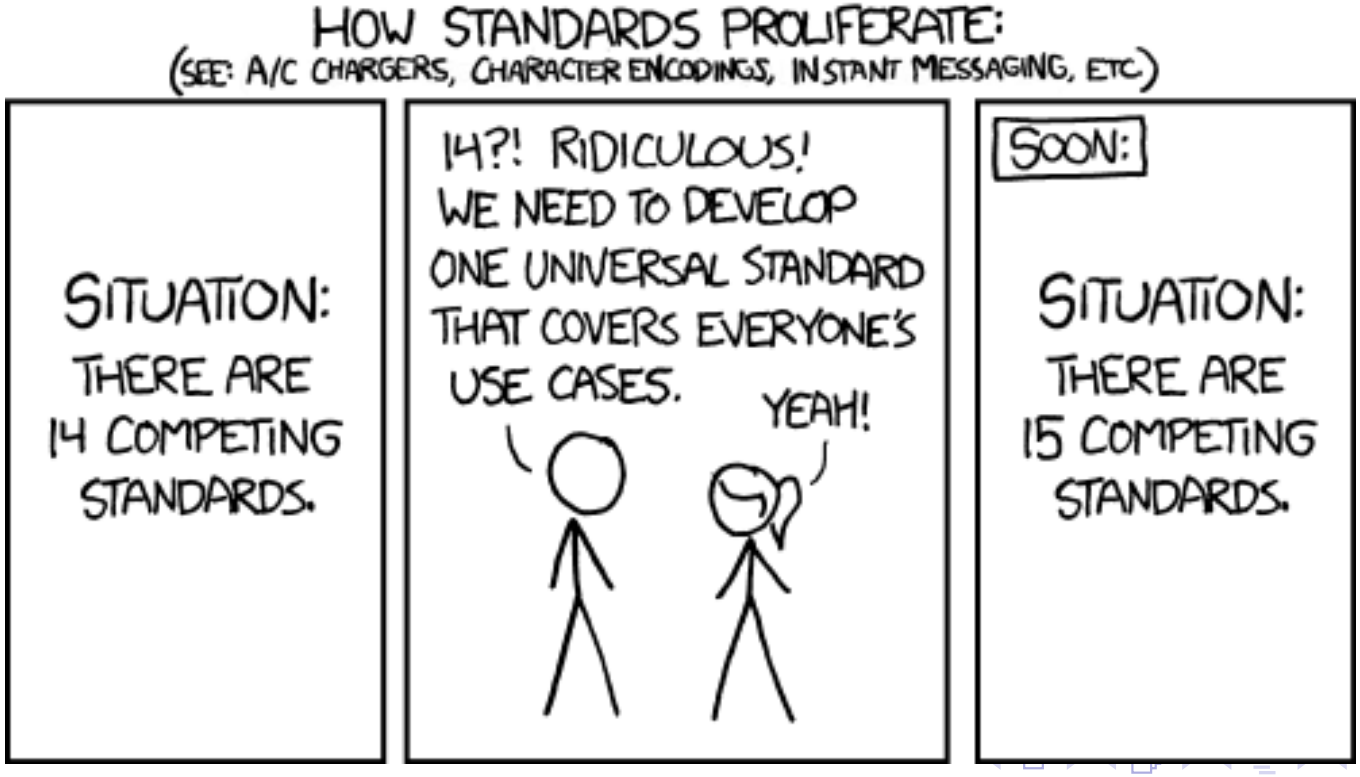
- Komplexitätstheorie der theoretischen Informatik
- maximaler Ressourcenbedarf eines Algorithmus
- idR Zeitkomplexität oder Platzkomplexität
- Landau-Symbol/Groß-O
  - Bubblesort: $\mathcal{O}(n^2)$
  - Mergesort: $\mathcal{O}(n \cdot \log(n))$
  - Bogosort: $\mathcal{O}(n \cdot n!)$
  - Slowsort: $\mathcal{O}\left(n^{\frac{\log(n)}{(2+e)}}\right)$



Komplexität

Soziologie

- soziale Komplexitätsreduktion gibt es nicht
- Standards sind etwas feines, jeder sollte einen haben ...



Komplexitätsreduktion

Soziologie

- OpenSSL Heartbleed
- OpenBSD forks, prunes, fixes OpenSSL $\rightsquigarrow$ LibreSSL
- Diskussion entsteht: Warum kein Komitee, dass die OpenSSL-Entwicklung steuert?
- Grundgesetz der Steuerungstechnik: Das steuernde System ist immer mindestens genau so komplex wie das zu steuernde System
- jedes neue Steuerelement führt weitere Komplexität ein
- und erhöht damit u.a. die Angreifbarkeit



Inhaltsverzeichnis

1 Vertrauen?

2 Komplexität

3 Sicherheit?

4 Schwachstelle Mensch?

5 Didaktik



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



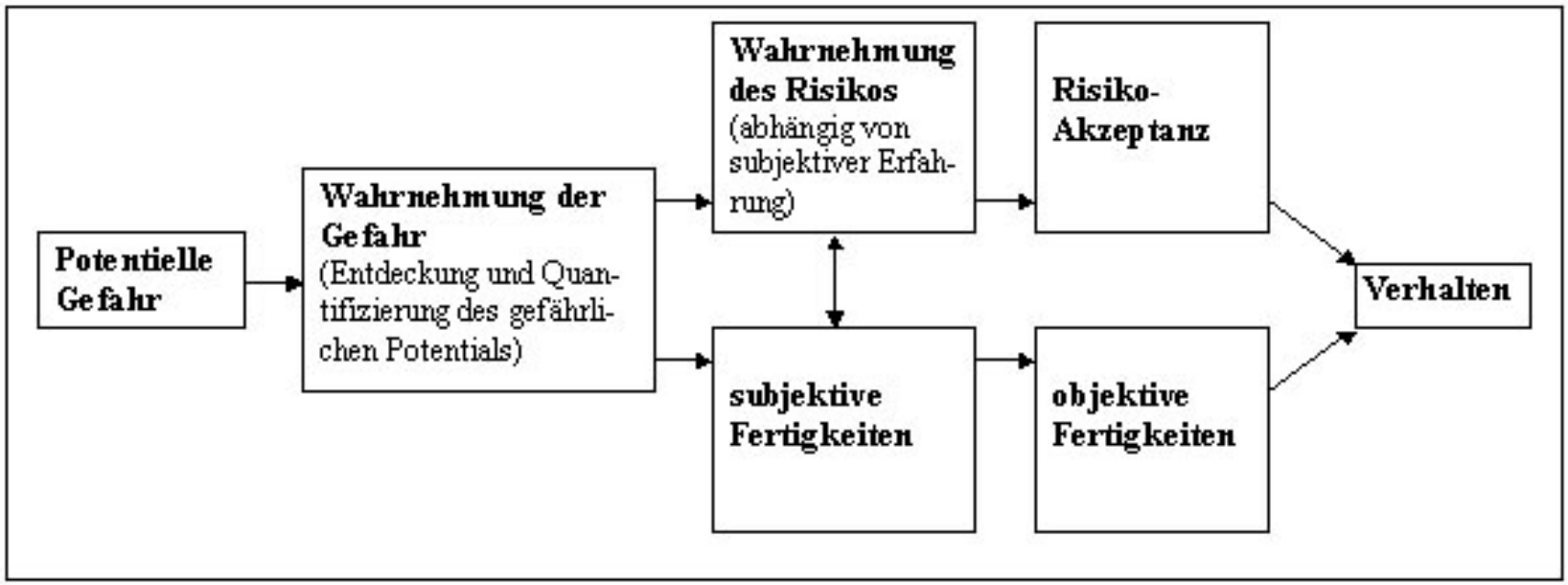
latentes soziales Konstrukt

- 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.



Risikohomöostasis

- Schutzmechanismen führen zur risikoaffinerem Verhalten
- Bsp: Fahrradhelm, Schutzkleidung, Daimler vs. Wolga



persönliche Konstruktion von Sicherheit

IT

- »Ich habe jetzt ein Apple MacBook. Damit bin ich sicher.«
- »Sie haben ja jetzt den Virenscanner der Uni installiert, da kann ich wieder auf die russischen Webseiten gehen.«
- »Auf Linux gibt es keine Viren!!!Eins!!ELF!!«



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 ...) ⇝ Spear Phishing

Inhaltsverzeichnis

1 Vertrauen?

2 Komplexität

3 Sicherheit?

4 Schwachstelle Mensch?

5 Didaktik



Schwachstelle Mensch?

- »Der Mensch ist die größte Schwachstelle in der IT-Sicherheit«
- Wirklich?
- Wer handelt denn?
- Computer können keine Entscheidungen treffen, nur Algorithmen abarbeiten
- Entscheidungen müssen vom Programmierer vorher getroffen werden
- Algorithmen (Berechnungsrahmen) müssen entwickelt werden
- die stumpfsinning abgearbeitet werden



Schwachstelle Mensch?

- »Der Mensch ist die größte Schwachstelle in der IT-Sicherheit«
- Wirklich?
- Wer handelt denn?
- Computer können keine Entscheidungen treffen, nur Algorithmen abarbeiten
- Entscheidungen müssen vom Programmierer vorher getroffen werden
- Algorithmen (Berechnungsrahmen) müssen entwickelt werden
- die stumpfsinning abgearbeitet werden



Schwachstelle Mensch?

- Computer (und Programme) können nicht entscheiden ob ein Vorgang sicherheitsgefährdend ist oder nicht, es sei denn es existiert ein Berechnungsrahmen dafür.
- Beispiel für Berechnungsrahmen: Eigenschaften eines sicheren Passworts, sichere Kryptoalgorithmen,
- d.h. der Sicherheitsvorfall ist trivial nach Heinz von Foerster
- über einen Berechnungsrahmen können Sicherheitsprobleme erkannt werden
- sofern dies algorithmisierbar ist
- algorithmisierbar heißt hier dass der Sicherheitsvorfall trivial ist
- z.B. bekannte und analysierte Viren



Handlung?

- alles was nicht algorithmisierbar/entscheidbar ist, muss von Menschen entschieden werden
- Nur Menschen können diese Entscheidungen treffen
- Menschen treffen Entscheidungen unbewusst oder bewusst
- Bewusst dann, wenn die Motivation dazu da ist
- und die Handlungskompetenz reicht



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



Inhaltsverzeichnis

1 Vertrauen?

2 Komplexität

3 Sicherheit?

4 Schwachstelle Mensch?

5 Didaktik

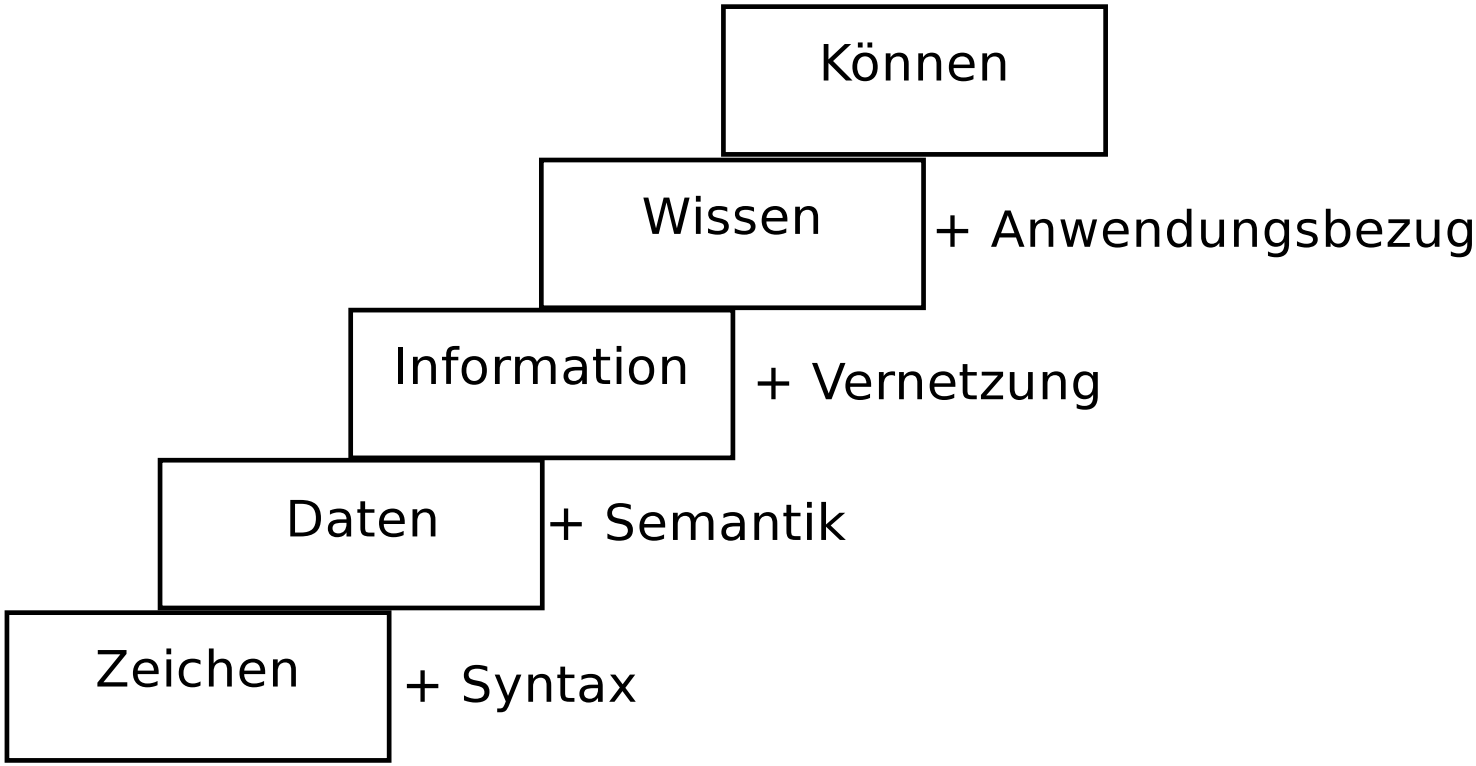


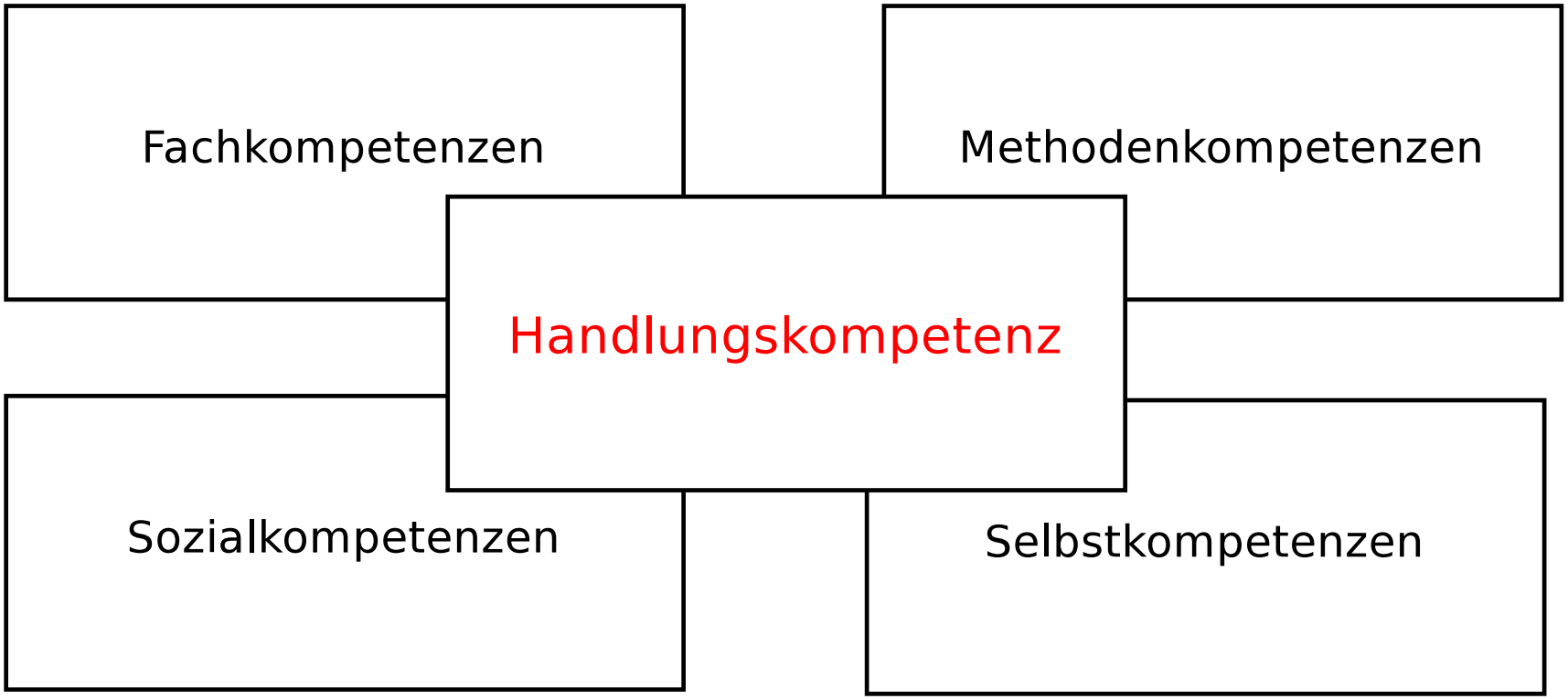
Didaktik der Sicherheit?

- Menschen müssen an/mit IT ausgebildet werden
- Didaktik der Sicherheit muss entwickelt werden
- Didaktik ist die Professionalisierungswissenschaft des Lehrers/Beraters
- Didaktik erforscht Methoden und Werkzeuge für Lehr-/Lernsettings
- Allgemeine Didaktik und Fachdidaktik z.B. für Schulfächer
- Ziel: Ausbildung von IT-Sicherheit im Kompetenzmodell der deutschen Berufsbildung



Wissenstreppe





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, ...
- Rollen in der IT-Sicherheit? (Admin, CISO, DBA, Anwender, Entwickler, Webmaster ...)
- Festlegung der Lerninhalte
- Möglichkeiten der Kompetenzdiagnostik?
- Zertifizierungen?



Literatur I

- Baecker, D. (2005a). Fehldiagnose überkomplexität. In D. Baecker (Hrsg.), *Organisation als System* (3. Aufl., S. 27–37). Frankfurt: Suhrkamp.
- Baecker, D. (Hrsg.). (2005b). *Organisation als System* (3. Aufl.). Frankfurt: Suhrkamp.
- Baecker, D. (2008). *Womit handeln Banken? Eine Untersuchung zur Risikoverarbeitung in der Wirtschaft* (7. Aufl.). Frankfurt: Suhrkamp.
- Beck, U. (1986). *Risikogesellschaft. Auf dem Weg in eine andere Moderne.*. Frankfurt: Suhrkamp.
- Beck, U. (2007). *Weltrisikogesellschaft: Auf der Suche nach der verlorenen Sicherheit*. Frankfurt: Suhrkamp.



Literatur II

- Cialdini, R. B. (2007). *Die Psychologie des überzeugens*. Bern (Schweiz): Verlag Hans Huber.
- Hacker, W. (2005). *Allgemeine Arbeitspsychologie* (2., vollst. überarb. u. erg. A.). Göttingen: Verlag Hans Huber.
- Luhmann, N. (2000). *Vertrauen* (4. Aufl.). Stuttgart: Lucius & Lucius / UTB.
- Luhmann, N. (2003). *Soziologie des Risikos* (unveränderter Nachdruck der Ausgabe von 1991). Berlin: Walter de Gruyter.
- Luhmann, N. (2008). *Legitimation durch Verfahren* (12. Aufl.). Frankfurt: Suhrkamp.
- Pias, C. (Hrsg.). (2009). *Abwehr: Modelle Strategien Medien* (1. Aufl.). Bielefeld: transcript.



Literatur III



Schumacher, S. (2011). Sicherheit messen: Eine Operationalisierung als latentes soziales Konstrukt. In S. Adorf, J.-F. Schaffeld & D. Schössler (Hrsg.), *Die sicherheitspolitische Streitkultur in der Bundesrepublik Deutschland: Beiträge zum 1. akademischen Nachwuchsförderpreis Goldene Eule des Bundesverbandes Sicherheitspolitik an Hochschulen (BSH)* (S. 1–38). Magdeburg: Meine Verlag. Verfügbar 11. November 2011 unter https://portal.dnb.de/opac.htm?method=simpleSearch&cqlMode=true&query=idn%3D1016863993



von Foerster, H. (1993). *Wissen und Gewissen: Versuch einer Brücke* (1. Aufl.). (S. J. Schmidt, Hrsg.). Frankfurt: Suhrkamp.

Literatur IV


Weizenbaum, J. (2003). *Die Macht der Computer und die Ohnmacht der Vernunft* (17. Aufl.). Frankfurt: Suhrkamp.

- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher