Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jörg Sambleben
Erschienen im Magdeburger Institut für Sicherheitsforschung

Dieser Artikel erscheint in der Serie „Informationstechnologie und Sicherheitspolitik. Wird der dritte Weltkrieg im Internet ausgetragen?“ Herausgegeben von Jörg Sambleben und Stefan Schumacher

Vom Cyber-Frieden

Stefan »Kaishakunin« Schumacher

Der Artikel beschreibt den ersten Entwurf einer Strategie zur globalen Cyber-Sicherheit. Dabei lege ich einen besonderen Schwerpunkt auf die Handlungskompetenz der handelnden Akteure und die zugrunde liegende psychologische Forschung.

Zitationsvorschlag: Schumacher, S. (2013). Vom Cyber-Frieden. *Magdeburger Journal zur Sicherheitsforschung*, *1*, 354–369. Zugriff 15. März 2013, unter http://www.sicherheitsforschung-magdeburg.de/publikationen.html

1 Einführung

Auch wenn es meiner Meinung nach keinen Cyber-Krieg *sui generis* gibt, ist und bleibt die IT-Sicherheit ein Feld, dem bereits jetzt schon eine hohe Bedeutung zu kommt. Fälle wie Stuxnet, Flame, Duqu und der Staatstrojaner haben gezeigt, welches Bedrohungspotenzial von Schadsoftware ausgehen kann. Durch die weitere Ausbreitung von Informationstechnologie in Kraftfahrzeuge und Industrieanlagen wird dieses Bedrohungspotenzial noch weiter erhöht.

Bisher wird das Problemfeld IT-Sicherheit nur unzureichend und eingeschränkt professionalisiert bearbeitet. Zwar hat sich die Informatik des Feldes IT-Sicherheit angenommen, aber naturgemäß (fast) nur aus technischer Sicht. Psychologie, Pädagogik und Soziologie sind aber ebenso notwendig um die IT-Sicherheit insgesamt zu erhöhen. Schließlich produzieren Menschen Software – und machen dabei die Fehler die zu Sicherheitslücken werden.

Als Beispiel sei hier nur der Buffer Overflow[1] genannt. Bereits der Morris-Wurm nutzte am 02.11.1988 einen Buffer-Overflow via `gets()` in finger(1) aus. 1996 beschrieb Aleph One in seinem Artikel *Smashing the Stack for Fun and Profit* Buffer Overflows ausführlich (Aleph One 1996). Die Maßnahmen gegen Buffer Overflows sind vergleichsweise einfach umzusetzen, selbst automatisierte Scanner[2], die Quellcode überprüfen existieren. Trotzdem kommt es immer noch und immer wieder zu Sicherheitslücken durch Buffer Overflows. So wurde im Frühjahr 2007 ein Buffer Overflow im IPv6 Kernel Modul von OpenBSD entdeckt[3] – einem Betriebssystem das besonderen Wert auf Sicherheit legt.

Das OpenBSD-Team hat auf diese Sicherheitslücke reagiert und eine aktualisierte Fassung des Quellcodes bereitgestellt. Allerdings löst dies nur diesen einen konkreten Buffer Overflow, nicht jedoch die Problematik der Buffer Overflows allgemein.

Daher möchte ich in diesem Aufsatz eine Strategie bzw. Doktrin als übergeordnete Richtlinie vorstellen, um die IT-Sicherheit allgemein zu erhöhen. Es geht dabei nicht so sehr um konkrete Ziele die innerhalb kurzer Zeit zu erreichen sind, sondern um Ziele deren Erreichen mehrere Zwischenziele voraussetzt.

Da es bereits umfangreiche und vorangeschrittene Entwicklungen im Bereich technische Sicherheit in der Informatik gibt und ich mich durch mein Studium der Bildungswissenschaft und Psychologie mit der menschlichen Seite von Sicherheit befasst habe, möchte ich diese auch näher beleuchten.

1 In meinem Kap. zu Schadsoftware näher erläutert

2 Stack Smashing Protector von IBM oder Stack Guard für die GCC.

3 http://www.coresecurity.com/content/open-bsd-advisorie v. 2007-03-15

2 Organisation? Virtuell!

Eine wirksame IT-Sicherheitsstrategie setzt eine globale Mitarbeit von vielen (relevanten) Akteuren voraus. Dazu gehören Software-Entwickler ebenso wie Systemadministratoren, Sicherheitsforscher, Juristen, Strafverfolgungsbehörden, Regierungen, NGOs, Endbenutzer und so weiter. Einige Organisationen die sich mit IT-Sicherheit befassen existieren bereits, beispielsweise das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die European Network and Information Security Agency (ENISA). Allerdings haben derartige Organisationen in der Regel eine recht starre Hierarchie, da sie als Bürokratie im Weberschen Sinne aufgebaut sind (Weber 1947a,b). Daher sind sie oft nur schwer in der Lage auf Veränderungen in der Umwelt zu reagieren und beispielsweise neue Akteure zu integrieren, ohne dass diese sich in das System der Behörde einpassen (vgl. Baecker 2005a; Luhmann 1999, 2008b).

Anstatt sich an einer formalen Behörde (also dem Bürokratieansatz) zu orientieren, sollte die Organisation einen anderen Ansatz verfolgen, den der virtuellen Organisation bzw. eines sogenannten Clusters of Competence. Dabei handelt es sich um einen formal losen Zusammenschluss von Experten zu einem bestimmten Thema, die bei Bedarf miteinander kommunizieren und Teams formieren um ein bestimmtes Problem zu lösen. Die Experten müssen nicht der selben formalen Organisation (Unternehmen, Universität, Behörde o.ä.) angehören, sondern lediglich Experte auf dem entsprechenden Gebiet sein. Die virtuelle Organisation formiert sich über technische Hilfsmittel, heutzutage insbesondere Kommunikationsmethoden im Internet wie Mailinglisten, Diskussionsforen oder speziellen Webseiten. Dabei entsteht ein dynamisches Netz mit schwach ausgeprägter Hierarchie, das in der Regel meritokratisch organisiert ist (vgl. Davidow und Malone 1992; Lemken und Cremers 1999; Nonaka und Takeuchi 1995; Scharmer 2007).

Musterbeispiele für derartige Organisationen sind Open-Source-Projekte[4]. Die meisten Projekte stellen über eine technische Infrastruktur Kommunikationsmethoden (E-Mail, Mailinglisten, Archive, CVS etc.) zur Verfügung. Die jeweiligen Entwickler (Experten) nutzen diese Methoden um das System weiter zu entwickeln oder um Probleme zu diskutieren und zu lösen. Dabei bilden sich Spezialisierungen der Expertengruppen heraus, beispielsweise Netzwerkentwickler, Kryptographen oder Administratoren der Entwicklungsserver. Raymond (1999) beschreibt diese Vorgehensweise in seinem bekannten Aufsatz und nennt das Entwicklungsmodell von Linux Basar, in Abgrenzung zu den hierarchischen Kathedralen der kommerziellen Softwareentwickler.

Neben der eigentlichen Entwicklungsarbeit bzw. Diskussion über IT-Sicherheit ist auch eine Kybernetik zweiter Ordnung sinnvoll. Von Foerster (1993a) bezeichnet die Kybernetik zweiter Ordnung als »Be-

4 Hubert Feyrer hat in seinem Kapitel »Sicherheit durch Freiheit« das NetBSD-Projekt näher beschrieben.

obachtung der Beobachtung«, die er als Eigenwertproblem der Kommunikation betrachtet. Bezogen auf Wissensmanagement kann man beispielsweise die Frage stellen, welchen Zweck der Zweck oder welches Ziel das Ziel hat.

Neben der Kybernetik zweiter Ordnung ist auch eine Diskursanalyse sinnvoll, in der wir selbst als Teil des Diskurses untersucht werden – also nicht einfach als »objektiver Beobachter« andere Diskurse analysieren, sondern selbst als Teil der Diskurses untersucht werden.

3 Vom Aussterben der Schadsoftware

In meinen beiden vorigen Kapiteln in diesem Buche spielt Schadsoftware eine große Rolle. Automatisierte Angriffe bzw. Angriffe über Schadsoftware machen einen Großteil aller Sicherheitsvorfälle aus. Verlässliche Zahlen existieren zwar nicht und sind auch kaum zuverlässig erhebbar, man kann aber mit großer Wahrscheinlichkeit von einer Art Pareto-Regel[5] ausgehen: 80% aller Sicherheitsvorfälle werden durch Schadsoftware und einfache Angriffe verursacht, lediglich 20% der Angriffe sind komlexer. Und 80% der Schadsoftware dürfte relativ einfacher Natur sein. Rottet man nun diese Schadsoftware aus, wäre ein Großteil aller Sicherheitsvorfälle vermieden. Daher sollte ein Ziel der globalen IT-Sicherheitsstrategie die Bekämpfung von Schadsoftware sein.

Vorbild für eine derartige Kampagne kann die Weltgesundheitsorganisation WHO sein. Es gelang ihr bereits 2 Krankheitserreger – Pocken und Rinderpest – auszurotten. Weil Sie dazu eine Strategie hatten.

Auch wenn es auf den ersten Blick größenwahnsinnig klingt, ist es durchaus möglich Schadsoftware auszurotten. Gegenüber der Weltgesundheitsorganisation hat die IT-Sicherheit einige Vorteile. Die »DNS« der Schädlinge ist bekannt beziehungsweise relativ leicht zu analysieren. Die mathematischen Konzepte der Informatik (Turing-Maschine, Algorithmus, Komplexitätsklassen etc.) sowie die meisten Sicherheitslücken sind bekannt und wohl erforscht. Außerdem werden Honeypots und Honeynets[6] eingesetzt um neue Angriffe zu enttarnen[7] und zu analysieren. Auf die Ergebnisse kann in der Sicherheitsforschung zurückgegriffen werden um zum einen auf taktischer Ebene die Sicherheitslücken zu stopfen, zum anderen können aber auch Rückschlüsse auf die strategische Ebene gezogen werden.

Ein weiterer großer Vorteil der IT-Sicherheit ist die relativ leichte Erreichbarkeit der »Patienten«. Niemand muss tagelang durch das Outback marschieren um zum Patienten zu kommen. Jeder Rechner der im Internet hängt und damit potenziell Opfer einer Attacke werden kann, kann über das Internet auch gepatcht und aktualisiert werden[8].

Das Ziel Schadsoftware auszurotten ist auf der strategischen Ebene angesiedelt. Es sind mehrere Zwischenschritte auf taktischer Ebene erforderlich. So ist es einstweilen sinnvoll, die Resilienz[9] von IT-Systemen zu erhöhen. Das heißt es ist notwendig, die Widerstandsfähigkeit beispielsweise durch Sandboxing, Virtualisierung oder Intrusion Detection Systeme auszubauen.

Abbildung 1 zeigt anhand einer Zeittafel die steigende Raffinesse von Angriffen auf IT-Sicherheitssysteme. Waren die ersten Angriffsmethoden wie Passwörter erraten in den 1980ern noch recht simpel, sind diese in den 2000ern wesentlich komplexer geworden. Dafür sanken die Fertigkeiten der Angreifer, da viele technische Angriffe inzwischen mittels vorhandener Software (»Skript«) von sogenannten Skript-Kiddies ausgeführt, die sich lediglich die fertigen Skripte verschaffen, um sie einzusetzen. Dadurch steigt die Zahl der Angriffe und Sicherheitsvorfälle von Jahr zu Jahr an, während gleichzeitig die technischen Voraussetzungen und intellektuellen Fähigkeiten auf Angreiferseite immer niedriger werden.

Ein erstes taktisches Ziel sollte es daher sein, die Attacken von Skript-Kiddies und einfacher Schadsoftware abzuwehren und somit die Angriffe mit geringer Komplexität (bzw. Angreifer mit niedriger Kompetenz) ins Leere laufen zu lassen. Dazu ist es zwingend notwendig, die Handlungskompetenz der Software-Entwickler, Administratoren und Anwender zu erhöhen. Wie dies möglich ist, werde ich im folgenden erläutern.

4 Sicherheit, Bewusstsein und Handlung: Psychologie der Sicherheit

Aus pädagogisch-psychologischer Sicht ist der erste Schritt im Problemfeld das Bewusstsein über IT-Sicherheit bei allen Betroffenen. Betroffen sind nicht nur Anwender, sondern auch Entwickler (inklusive Projektmanager und derjenigen, die das Requirements Engineering durchführen und Projektziele festlegen), Kunden und Politiker. Ohne Sicherheitsbewusstsein wird Sicherheit nicht als relevant wahrgenommen, handelnde Individuen sind daher nicht motivier, Sicherheit bei ihren Handlungen als notwendigen Faktor zu betrachten. Daher ist es zwingend notwendig Sicherheit als relevant für handelnde Individuen

Hersteller von IT-Systemen müssen IT-Sicherheit als Entwicklungsziel priorisieren. Es geht nicht, Sicherheit nicht oder kaum zu beachten. Es ist auch nicht

5 Auch 80/20-Regel genannt.

6 http://project.honeynet.org/ v. 2012-10-22

7 http://www.shadowserver.org/ v. 2012-10-22

8 Eine derartige Update-Funktion kann natürlich auch wieder gehackt und missbraucht werden. Man könnte darüber einen Root-Zugang und Millionen von Systemen installieren. Daher wäre der Hack eines Update-Systems sozusagen der Heilige Gral der Angreiferszene.

9 Der Begriff wird im Punkt *Organisationssicherheit* näher besprochen.

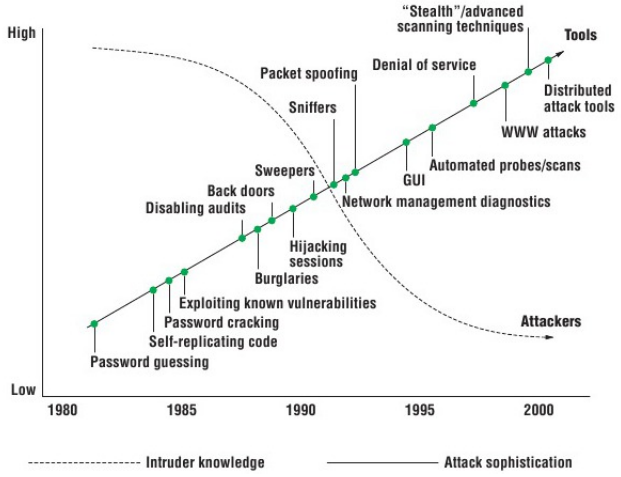

Abbildung 1: Angriffs-Komplexität und Angreiferfertigkeiten Quelle: Allen u. a. (2000, Seite 43)

akzeptabel Sicherheit als Add-On-Feature zu verkaufen[10].

Käufer von IT-Systemen müssen ebenfalls IT-Sicherheit priorisieren. Nur so ist es möglich, Hersteller ebenfalls von der Wichtigkeit der Sicherheit zu überzeugen. Solange Smartphones nur anhand der Auflösung der eingebauten Kameras[11] bewertet werden, wird Sicherheit schon aus Kostengründen keine Rolle spielen. Käufer haben aber eine entsprechende Marktmacht: wenn sie nur noch Produkte mit adäquatem Sicherheitsniveau erwerben möchten, werden sich die Hersteller nach diesem Wunsch richten und entsprechende Systeme anbieten müssen.

Allerdings muss ich auch einräumen, dass es eher unrealistisch ist, anzunehmen die Konsumenten würden bei Smartphones in Zukunft Sicherheit priorisieren. Daher kann es auch sinnvoll sein im Rahmen der nationalen oder internationalen Gesetzgebung Sicherheit von den Herstellern von IT-Systemen zu verlangen. Schließlich müssen auch die Hersteller von Flugzeugen, Autos oder medizinischen Geräten vielfältige Sicherheitsvorschriften beachten und umsetzen. So musste Toyota 2010 mehrere Millionen PKW zurückrufen, da es Probleme mit dem Gaspedal[12] gab - ein Rückruf von Betriebssystemen ist mir bisher nicht bekannt.

Politiker sind nicht nur im Problemfeld Cyberwar oder Staatstrojaner mit dem Bereich IT-Sicherheit konfrontiert, daher ist es zwingend notwendig, Politiker und andere Entscheidungsträger entsprechend zu beraten und sie mit den notwendigen technischen Hintergrundinformationen und Technikfolgeabschätzungen zu versorgen.

10 Bitlocker ist beispielsweise nur für Windows 7 Ultimate und Enterprise erhältlich, nicht jedoch für Home.

11 Die verbauten Kameras sind eh von bescheidener Qualität und die Auflösung des Sensors ist nicht das alleinige Qualitätskriterium.

12 http://www.auto-motor-und-sport.de/news/toyota-rueckruf-alle-infos-zum-toyota-gaspedal-rueckruf-1721119.html v. 2011-07-07

5 Der Sicherheits-Begriff und Sicherheit in anderen Bereichen

Zuerst möchte ich den Begriff der Sicherheit explizieren, da es notwendig ist, das dahinterliegende Konzept zu explizieren.

Die Aussage, *etwas ist sicher*, beschreibt eine Anforderung an eine Sache oder einen Zustand. Es beschreibt, wie etwas sein soll. Es ist also eine *normative Aussage*. Damit aus der Beschreibung, der Deskription, einer Sache oder eines Zustandes eine Bewertung erfolgen kann, sind Bewertungsgrundsätze, sogenannte *Prämissen* erforderlich. Eine Bewertung ohne Prämisse ist ein naturalistischer Fehlschluss und daher unzulässig.

Diese Prämissen können aus Erfahrung heraus (a posteriori) oder unabhängig von Erfahrung (a priori) festgelegt werden. Sie legen damit fest, wie die Merkmale einer Sache zu sein haben, damit die Sache als sicher bezeichnet werden kann. Im Rahmen einer Diagnose werden die Prämissen auf eine Sache angewendet, die Sache wird daraufhin in die Klasse sicher oder unsicher eingeteilt (vgl. Poser 2001, Seiten 27 ff.).

Das heißt bezugnehmend auf von Foerster (1993b, S. 340), dass die Prämissen eine Maschine erzeugen, die die Sicherheit einer Sache berechnbar macht. Ich stelle daher fest, das der Begriff Sicherheit *normativer* Natur ist:

- α. Die Aussage etwas ist sicher ist eine normative Aussage.
- β. Damit diese normative Aussage getroffen werden kann, ist eine Prämisse notwendig. Diese Prämisse heiße *Diagnosekriterium*.
- γ. Ein Diagnosekriterium kann a priori oder a posteriori festgelegt werden.
- δ. Die Menge aller Diagnosekriterien legt fest wie etwas zu sein hat, damit es als sicher bezeichnet werden kann.
- ε. Die Anwendung der Diagnosekriterien auf eine Sache heiße *Sicherheitsdiagnose*.

ζ. Die Anwendung der Sicherheitsdiagnose scheide Sachen in die Klassen sicher und unsicher.

Diese Vorgehensweise ist auf verschiedene Sicherheitsbegriffe anwendbar und prinzipiell auch auf andere normative Begriffe übertragbar, da sie eine grundlegende Methode zum Umgang mit Bewertungen darstellt.

Es ist nun notwendig, geeignete Bewertungsprämissen für den Begriff der Sicherheit zu explizieren. Dazu möchte ich zuerst Sicherheitsbegriffe aus anderen Gebieten vorstellen.

Diese Vorgehensweise ist auf verschiedene Sicherheitsbegriffe anwendbar und prinzipiell auch auf andere normative Begriffe übertragbar, da sie eine grundlegende Methode zum Umgang mit Bewertungen darstellt.

Es ist nun notwendig, geeignete Bewertungsprämissen für den Begriff der Sicherheit zu explizieren. Dazu möchte ich zuerst Sicherheitsbegriffe aus anderen Gebieten vorstellen.

Die Norm *DIN EN 61508 / VDE 0803: Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme* (2002) definiert »Sicherheit« für elektrische Systeme als Freiheit von unvertretbaren Risiken. Hier ist die Freiheit von unvertretbaren Risiken das Diagnosekriterium, welches aber selber noch genauer expliziert oder definiert werden muss, denn sowohl »Risiko« als auch »unvertretbar« sind wertende Aussagen und benötigen daher eine Bewertungsprämisse. Dies wird im Rahmen der DIN-Norm auch getan, in dem beispielsweise die Wahrscheinlichkeit des Versagens eines Gerätes pro Stunde als Kriterium definiert wird. Es werden in der DIN-Norm also geeignete Prämissen und Messverfahren vorgestellt, die einen Rahmen zur Messung des Begriffs Sicherheit bieten.

Die Elektrosicherheit hat gegenüber der IT-Sicherheit aber den entscheidenden Vorteil der geringeren Mensch-Maschine-Interaktion und Veränderbarkeit der Software. Ein Computernutzer kann wesentlich stärker mit einem Computer interagieren und ihn verändern. Der Nutzer einer Bohrmaschine kann diese nur sehr beschränkt manipulieren und damit unsicherer machen. Er könnte sie zwar von einer Leiter aus fallen lassen und das doppelte Gehäuse beschädigen. Damit wäre die Elektrosicherheit eingeschränkt, da ein Kontakt zwischen elektrischem Leiter und Anwender möglich ist. In der Regel wird solch ein Fall aber durch Sicherheitshinweise im Handbuch ausgeschlossen. So enthält jedes Handbuch für ein elektrisches Gerät den Hinweis, dass es nicht vom Anwender geöffnet werden dürfe. Damit ist zumindest aus rechtlicher Sicht der Hersteller bzw. Verkäufer abgesichert.

Im Maschinenbau gelten ähnlich wie in der Elektrotechnik DIN-Normen, die beispielsweise Belastungsgrenzen oder Maßvorgaben festlegen. So legt die *DIN EN ISO 13857: Sicherheit von Maschinen - Sicherheitsabstände gegen das Erreichen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen* (2008) unter anderem fest, welche Mindestbreite Spalten haben müssen, damit sich ein Maschinenbediener nicht quetschen kann. Die notwendigen Maße werden in der Regel experimentell bestimmt und beispielsweise bei neuartigen Maschinen oder nach statistischer Auswertung der meldepflichtigen Arbeitsunfälle neu berechnet. Ebenso werden Belastungstests mit Maschinen durchgeführt, aus denen dann Belastungssgrenzen abgeleitet werden. Die Prämissen der Sicherheit werden hier also in der Regel experimentell bestimmt oder durch experimentell generierte mathematische Formeln berechnet. Genügt eine Maschine diesen Regeln, wird sie als sicher eingestuft und darf genutzt werden.

In der Informatik bzw. der IT-Sicherheit werden verschiedene Diagnosekriterien festgelegt, die der Sicherheitsdiagnose von Software, Hardware und ganzen IT-Systemen dienen. Am bekanntesten sind die sogenannten VIVA-Kriterien, also Vertraulichkeit, Verfügbarkeit, Integrität und Authentisierung, welche unter anderem vom Bundesamt für Sicherheit in der Informationstechnik (2006) wie folgt definiert werden:

Vertraulichkeit Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

Integrität Die Daten sind vollständig und unverändert. Der Begriff »Information» wird in der Informationstechnik für »Daten« verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.

Verfügbarkeit Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.

Authentisierung Bei der Anmeldung an einem System wird im Rahmen der Authentisierung die Identität der Person, die sich anmeldet, geprüft und verifiziert. Der Begriff wird auch verwendet, wenn die Identität von IT-Komponenten oder Anwendungen geprüft wird. Ist die Authentisierung erfolgreich, spricht man auch davon, dass die Person oder ein Datum authentisch ist bzw. die Authentizität gewährleistet ist.

6 Handlungen, Fähigkeiten, Fertigkeiten und Kenntnisse

IT-Sicherheit ist nicht-trivial und multi-dimensional, das heißt sie kann nicht einfach berechnet werden und sie findet in der technischen, psychischen und sozialen Dimension statt. In der psychischen Dimension hängt IT-Sicherheit von der Entscheidung bzw. dem Verhalten von Individuen ab. Daher werde ich in diesem Kapitel menschliches Verhalten in Bezug auf *Sicherheit* näher untersuchen. Fraglich ist hierbei,

ob und wie sich menschliches Verhalten messen und vorhersagen lässt, welche Werkzeuge und Methoden dazu bereits existieren und wie sich diese gegebenenfalls im Bereich IT-Sicherheit nutzen lassen.

Die Arbeitspsychologie nutzt zur Beschreibung und Prognose menschlicher Handlungen sogenannte Handlungsregulationstheorien und Kompetenzmodelle. Mit diesen Modellen lassen sich Handlungen beschreiben, sowie Handlungen mithilfe eines Bewertungsrahmens diagnostizieren und prognostizieren.

Der erste wichtige Punkt einer Handlung bezogen auf Sicherheit ist hierbei die Antizipation eines zukünftigen Ereignisses als gefährlich: Sicherheit wird in der Regel als *Freiheit von unvertretbaren Risiken* definiert, (vgl. Deutsches Institut für Normung 2002).

Nach Beck (2007, Seite 29) bedeutet Risiko

> die *Antizipation*[13] der Katastrophe. Risiken handeln von der Möglichkeit künftiger Ereignisse und Entwicklungen, sie vergegenwärtigen einen Weltzustand, den es (noch) nicht gibt. Während jede Katastrophe räumlich, zeitlich und sozial bestimmt ist, kennt die Antizipation der Katastrophe keine raum-zeitliche oder soziale Konkretion. [...] Risiken sind immer *zukünftige* Ereignisse, die uns *möglicherweise* bevorstehen, uns *bedrohen*.

Das handelnde Individuum muss also Ereignisse, die in der Zukunft *wahrscheinlich* eintreten und *wahrscheinlich* schädlich sind bei der jetzigen Regulation seiner Handlungen einbeziehen. Übertragen auf einen kybernetischen Regelkreis wirkt also ein angenommenes Ereignis in der Zukunft auf die Gegenwart zurück und beeinflusst aktuelle Entscheidungen des Individuums (vgl. dazu insbesondere Schumacher 2010).

Ziel des folgenden Kapitels ist es daher, individuelle Entscheidungen und Handlungen zu modellieren und geeignete Prognose- und Interventionsmethoden zu finden.

Für die Arbeitspsychologie hat insbesondere Hacker (2005, Seite 63) die Grundlagen der psychischen Regulation von Arbeit gelegt. Er definiert dabei die Aufgabe als Übernahme eines »objektiven Arbeitsauftrages«, der einer Aufgabe Sinn verleihe. Sie sei daher nicht nur ein psychologischer Auftrag, sondern auch ein rechtlicher und betriebswirtschaftlicher Sachverhalt, der beispielsweise die Lohnzahlung begründe.

Die *Aufgabe* ist somit eine der fundamentalen Grundlagen der Arbeitspsychologie. Sie ist aber im Rahmen dieser Sicherheitsdiskussion nur beschränkt sinnvoll einsetzbar, da IT-Sicherheit in der Regel kein expliziter Arbeitsauftrag ist, sondern in der Regel implizit erteilt wird. Ein Finanzbuchhalter soll vorrangig buchführen, ein Webredakteur soll die Webseite betreuen. IT-Sicherheit ist daher keine wirklichen »Aufgabe« ihrer Tätigkeit. Lediglich für einen Systemadministrator, der den Auftrag hat die Sicherheit eines IT-Systems zu untersuchen, kann IT-Sicherheit zur expliziten Aufgabe werden. Für alle anderen ist IT-Sicherheit »nur« eine implizite Nebenaufgabe zu ihren Hauptaufgaben. Es sind also weitere Konstrukte notwendig.

Diese finden sich in der *Handlung* und der *Operation*, die nach Hacker (2005, Seiten 68 ff.) wie folgt definiert werden: »*Handlung*[14] bezeichnet nämlich eine in sich geschlossene Einheit der Tätigkeit. [...] Die umfassenderen Vollzüge seien als Tätigkeit bezeichnet.« Operationen sind dagegen »nur unselbständige Bestandteile der Tätigkeit, da ihre Resultate nicht bewusst (als Ziel) antizipiert werden. Vielmehr werden sie durch *Auslösebedingungen* reguliert [...]«. Man kann also die sicherheitsrelevanten Teile einer Tätigkeit entweder als Handlung (wenn sie bewusst gesteuert wird) oder als Operation betrachten, die durch Auslösebedingungen unselbständig ausgeführt werden.

Aufbauend auf der Handlungsregulationstheorie wurde unter anderem in der Pädagogik das Konzept der Fähigkeiten, Fertigkeiten und Kenntnisse eingeführt.

Erpenbeck und Sauter (2007, S. 67f) definieren diese wie folgt:

> *Fähigkeiten* bezeichnen verfestigte Systeme verallgemeinerter psychophysischer Handlungsprozesse einschließlich der zur Ausführung einer Tätigkeit oder Handlung erforderlichen inneren physischen Bedingungen und der lebensgeschichtlich unter bestimmten Anlagevoraussetzungen erworbenen Eigenschaften, die den Tätigkeits- und Handlungsvollzug steuern.
>
> *Fertigkeiten* bezeichnen durch Übung automatisierte Komponenten von Tätigkeiten, meist auf sensumotorischen Gebiet, unter geringer Bewusstseinskontrolle, in stereotypen beruflichen Anforderungsbereichen, auch im kognitiven Bereich [...]. Fertigkeiten haben das individuelle Verhalten, den psychophysischen Tätigkeits- und Handlungsprozess als Ganzes im Blick. Sie sind handlungszentriert. [...] Der Erwerb einer Fertigkeit ist nicht ausschließlich von Begabungen und Talenten abhängig, sondern auch von Übung, von anderen bereits erlernten Fertigkeiten, von Kenntnissen und Erfahrungen.

Wissen wird an selber Stelle als »die auf Begründungen bezogene und strengen Überprüfungspostulaten unterliegende Kenntnis, institutionalisiert im Rahmen der Wissenschaft« definiert.

Fähigkeiten, Fertigkeiten und Kenntnisse stellen also die grundlegenden Voraussetzungen für eine Handlung dar, die gewissen von außen herangetragenen Kriterien genügen muss. Es ist beispielsweise Aufga-

13 Hervorhebungen im Original [SS]

14 Hervorhebungen im Original [SS]

be der Berufsausbildung, verschiedene in den Rahmenlehrplänen festgelegte Fähigkeiten, Fertigkeiten und Kenntnisse zu vermitteln.

Aber bereits in der Diskussion um das Konzept der *Schlüsselqualifikationen* zeigte sich, dass Fähigkeiten, Fertigkeiten und Kenntnisse in der Berufsbildung alleine nicht ausreichen, da sie zwar Wissen vermitteln, nicht aber den Umgang *mit* Wissen. Daher wurde der Begriff der Schlüsselqualifikation eingeführt, der unter anderem den selbständigen Erwerb neuen Wissens beinhaltet. Dies sollte dem Obsoleszenzproblem und Prognoseproblem entgegenwirken, da zur Zeit der Berufsausbildung nicht klar war, in welcher Arbeitswelt sich der Berufsschüler zurechtfinden muss. Das damals gelehrte Wissen veraltete relativ schnell (wurde obsolet) und es war nicht klar, welches Wissen in Zukunft notwendig werden würde (Prognose) (vgl. Mertens 1974). Diese Entwicklung wurde durch die Automatisierung und PC-Revolution nocht dramatisch verschäft, so sind beispielsweise die Berufe Kfz-Mechaniker, Kfz-Elektriker und Automobilmechaniker 2001 zum wesentlich komplexeren Beruf Kfz-Mechatroniker neu geordnet worden.

Das Konzept der Schlüsselqualifikationen wiederum wurde später zum Kompetenzbegriff erweitert, welcher im folgenden Kapitel untersucht wird. Er umfasst ein weitergehenderes Handlungskonzept, unter anderem durch die Einbindung von Motivation, und ist damit geeigneter als das Konzept der Fähigkeiten, Fertigkeiten und Kenntnisse. Am Ende des Kapitels werde ich diese Aussagen durch ein Anwendungs-Beispiel belegen.

7 Kompetenz

Den einen Kompetenzbegriff gibt es ebensowenig wie es den einen Wissensbegriff gibt. Die Kompetenzdiskussion hat in der deutschen Arbeitspsychologie und Berufspädagogik zu verschiedenen Kompetenzbegriffen und -definitionen geführt.

So definiert Gessler (2006, S. 26): »Kompetenz befähigt einen Menschen zu selbstverantwortlichem Handeln und bezeichnet den tatsächlich erreichten Lernerfolg. Qualifikation ermöglicht die Verwertung von Kenntnissen, Fertigkeiten und Fähigkeiten«.

Kauffeld u. a. (2003, S. 261) definieren berufliche Handlungskompetenz als »alle Fähigkeiten, Fertigkeiten, Denkmethoden und Wissensbestände des Menschen, die ihn bei der Bewältigung konkreter sowohl vertrauter als auch neuartiger Arbeitsaufgaben selbstorganisiert, aufgabengemäß, zielgerichtet, situationsbedingt und verantwortungsbewusst – oft in Kooperation mit anderen – handlungs- und reaktionsfähig machen und sich in der erfolgreichen Bewältigung konkreter Arbeitsanforderungen zeigen, verstanden.«

Staudt u. a. (2002, S. 440) legen in ihrer Kompetenzdefinition sogar Wert darauf, das Kompetenz der Schlüssel zur Innovation sei, und damit Voraussetzung um, »neue Sach- und Dienstleistungen, Materialien und Verfahren zu entwickeln und in wirtschaftliche Erfolge umzusetzen«. Außerdem seien sie ein wichtiger Faktor in der Unternehmensentwicklung, in dem sie zum einen durch Kompetenzdefizite die Weiterentwicklung des Unternehmens begrenzen, zum anderen aber auch Unternehmensentwicklung durch die Erschließung neuer Möglichkeiten ermöglichen. Sie betrachten die Kompetenzen also eher aus unternehmerischer Sicht, legen aber dabei dar, das die Entwicklung der Organisation von den Kompetenzen der Mitarbeiter abhängt. Dieser Punkt wird später in der Diskussion um Sicherheit als Dimension der Organisation eine Rolle spielen.

Im Rahmen meiner Hausarbeit zu sozialen Kompetenzen (Schumacher 2008) habe ich mich eingehender mit dem Kompetenzbegriff von Kanning (2007, S. 14) befasst. Er schreibt: »*Kompetenzen*[15] versetzen einen Menschen potenziell in die Lage, eine bestimmte Aufgabe erfolgreich lösen zu können. Zu einer tatsächlichen Lösung der Aufgabe kommt es jedoch erst dann, wenn die Kompetenzen in *Verhalten* umgesetzt werden.«

Dieser Kompetenzbegriff ist zwar unschärfer als die vorigen Definitionen, ermöglicht genau dadurch aber eine bessere Anpassung an spezifische Anforderungen, die ich im folgenden Vornehmen werde. Wichtig in dieser Definition ist die Tatsache, dass Kompetenz ein Potenzial darstellt, das heißt, Kompetenzen befähigen dazu, einen Akt auszuführen. Kompetenz bedeutet aber noch nicht, dass dieser Akt auch ausgeführt wird. Erst im Akt der *Handlung* zeigt sich die Anwendung der Kompetenzen, und auch nur dann, wenn die Aufgabe erfolgreich gelöst wurde, die Handlung also *kompetent* war.

Abbildung 3 zeigt den Zusammenhang zwischen Kompetenz und Verhalten, der nach Kanning (2007, S. 15) für das Verständnis von sozialer Kompetenz unerlässlich sei. So würde Motivation und Befindlichkeiten des Individuums sein kompetentes Verhalten ebenso beeinflussen wie Zeitdruck und das Verhalten anderer. Derartige Aussagen finden sich in allen anderen mir bekannten Kompetenzmodellen, das sich Kanning hier aber im Rahmen der sozialen Kompetenzen direkt auf soziale Interaktion bezieht, bieten sich seine Begriffe für eine Diskussion des Social Engineerings besonders an.

Abb. 2 zeigt die Wissentreppe[16] von North (2002), in der die Stufen einer kompetenten Handlung gezeigt werden. Die ersten 4 Stufen (Zeichen, Daten, Informationen, Wissen) stellen die Grundlagen der kompetenten Handlung dar, also Fähigkeiten, Fertigkeiten und Kenntnisse. Diese Fähigkeiten, Fertigkeiten und Kenntnisse müssen vom Individuum in einen Anwendungsbezug gesetzt werden. Zusammen mit diesem Anwendungsbezug ergibt sich das Können, also das *Potenzial* etwas zu tun. Das Potenzial muss dann durch Wollen, also Motivation, in eine Handlung um-

15 Hervorhebungen im Original [SS]

16 Ich habe die Punkte zum organisationalen Wissensmanagement und zum Unternehmenserfolg entfernt, da diese hier in der Diskussion persönlicher Kompetenzen keine Rolle spielen.

gesetzt werden. Die Handlung ist der Akt, in dem sich die vorhergehenden Stufen, also das Potenzial, zeigt und messbar wird. War die Handlung richtig, können wir von einer kompetenten Handlung sprechen. Kompetenz ist also nur in der konkreten Handlung messbar, und dann auch nur ex post.

Es bleibt also hervorzuheben, das Kompetenzen an sich nur ein Handlungspotential, also *Dispositionen* sind. Weiterhin sind Kompetenzen nur nach vollendeter Handlung, also ex post messbar. Erst die vollbrachte Handlung löst dabei eine gestellte Aufgabe erfolgreich.

In der Praxis hat sich dazu folgende 4-Teilung bzw. Dimensionierung von Kompetenzen durchgesetzt (nach Erpenbeck und von Rosenstiel 2007, Seite XXIV):

Fachkompetenz selbstorganisiertes Handeln, Motive, Werthaltung, Selbstbild, produktive Einstellung

Sozialkompetenz kommunikatives und kooperatives Handeln, gruppen- und beziehungsorientiertes Verhalten, Entwicklung neuer Pläne, Werthaltungen und Ziele.

Selbstkompetenz selbstorganisiertes, reflexives Handeln einer Person, eigene Begabungen, Motivationen entfalten

Methodenkompetenz selbstorganisiert gesamtheitlich und aktiv handeln, eigene Handlungen auf die Umsetzung von Vorhaben und Pläne richten

Zeigt ein Individuum in allen 4 Dimensionen kompetentes Verhalten, kommt es zur sogenannten *Handlungskompetenz*. Sekretariat der Kultusministerkonferenz (2007) definiert daher Handlungskompetenz als »die Fähigkeit des Einzelnen sich in beruflichen, gesellschaftlichen und privaten Situationen sachgerecht, durchdacht, sowie individuell und sozial verantwortlich zu verhalten«.

Handlungskompetenz ist daher das höchste Ziel der Berufsausbildung bzw. jeder Kompetenzentwicklungsmaßnahme überhaupt.

Das Kompetenzmodell wird zur Zeit sowohl in der Berufspädagogik (vgl. Sekretariat der Kultusministerkonferenz 2007), in der Grundschulpädagogik (vgl. Landesinstitut für Schule und Medien Berlin-Brandenburg 2007) als auch in der Arbeitspsychologie und Eignungsdiagnostik (vgl. Langens u. a. 2003) umfassend eingesetzt.

Es bietet sich daher auch für die Messung der psychischen und sozialen Dimension von IT-Sicherheit an, da die wissenschaftlich entwickelten Kompetenzmodelle sowohl Messung von Kompetenzen als auch Entwicklung von Kompetenzen ermöglichen – also sehr gut ausgearbeitete Methoden der Prognose, Diagnose und Intervention bieten. Sie müssen »nur« noch auf das Anwendungsgebiet IT-Sicherheit bzw. Organisationssicherheit übertragen werden.

Die deutsche Kompetenzforschung stellt damit sowohl wissenschaftlich fundierte, als auch praktisch erprobte Kompetenzmodelle und Messmethoden zur Verfügung. Da der Einsatz eines konkreten Kompetenzmodells immer vom Zweck und der Organisation selbst abhängt, kann und wird es das eine Kompetenzmodell für IT-Sicherheit nicht geben. Stattdessen kann man einzelne Kompetenzmodelle wie das Multi-Motiv-Gitter (Langens u. a. 2003) für spezifische Fragestellungen, zum Beispiel die Ausprägung einzelner Motive eines Mitarbeiters, einsetzen.

Man wird aber nicht umhin kommen, für jede Organisation ein, oder sogar mehrere, passende Kompetenzmodelle zu entwickeln. Diese müssen den jeweiligen Anforderungen angepasst und adäquat evaluiert werden.

7.1 Sicherheitskompetenz

Im vorhergehenden Kapitel habe ich gezeigt, dass Sicherheitskompetenz einen Bewertungsrahmen benötigt, um gemessen werden zu können. Dieser Bewertungsrahmen lässt sich in in zwei fundamental unterschiedliche Arten unterteilen: das Ergebnis ist bekannt und das Ergebnis ist unbekannt.

Beide Fälle unterscheiden sich nicht einfach nur darin, dass das Ergebnis bekannt ist, sondern erfordern eine andere intellektuelle Regulation im Individuum und eine andere Anwendung des Kompetenzbegriffs, und auch konsequenterweise andere didaktische Methoden (vgl. v. a. Hacker 2005).

Ist das Ergebnis der Handlung bekannt, weil es beispielsweise durch die anzuwendenden technischen Geräte determiniert ist oder weil eine hinreichend bekannte und vergleichsweise einfach nachzuvollziehende Sicherheitsrichtlinie existiert, ist die kompetente Handlung im Prinzip vorherbestimmt, also determiniert. Es kommt nun »nur« noch darauf an, diese Handlung vom Individuum adäquat umsetzen zu lassen.

Ist das Ergebnis der Handlung hingegen unbekannt, kommt es darauf an, dass das Individuum in der Handlung die *richtigen* Entscheidungen trifft. Dabei muss es selbständig entscheiden, welche Entscheidung es trifft. Diese Entscheidung ist ebenfalls erst wieder ex post analysierbar, manchmal mit erheblichem Zeitverzug und in Kombination mit der Handlung *anderer* Personen. Das Individuum muss sich dazu selbst beobachten, also Kybernetik 2. Ordnung betreiben (vgl. von Foerster 2008).

Ich möchte dies an einem Beispiel verdeutlichen: Alice soll für ein Benutzerkonto ein neues Passwort vergeben. Die Sicherheitsrichtlinie in ihrer Organisation schreibt gewisse Kriterien für die Güte eines Passwortes vor: es hat mindestens 10 Zeichen lang zu sein und je mindestens 2 Groß- und Kleinbuchstaben, 2 Sonderzeichen und 2 Ziffern zu enthalten, außerdem ist es geheimzuhalten. Somit ist für Alice das Auswahlkriterium für ein sicheres Passwort klar, die Wahl des Passwortes damit determiniert. Jede Handlung, bei der sie ein Passwort setzt, dass diesen Kriterien genügt, ist damit eine kompetente Handlung.

Ebenso verhält es sich sich, wenn Alice ihr Passwort

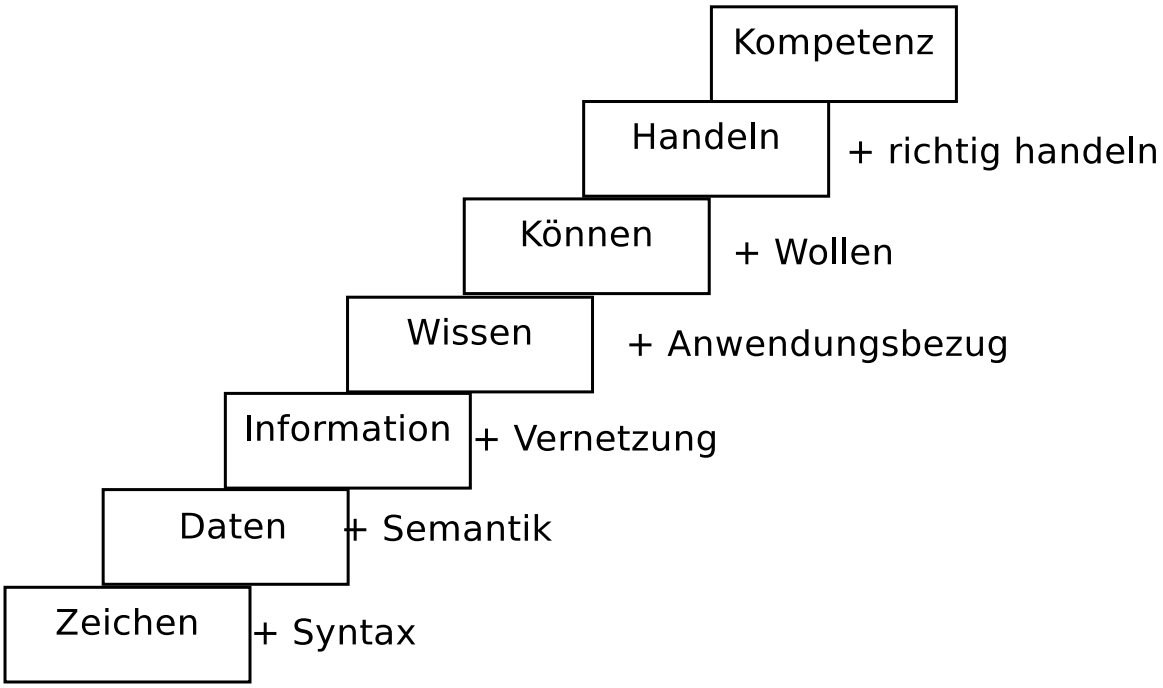

Abbildung 2: Wissenstreppe nach North (2002); selbsterstellte, gekürzte Darstellung

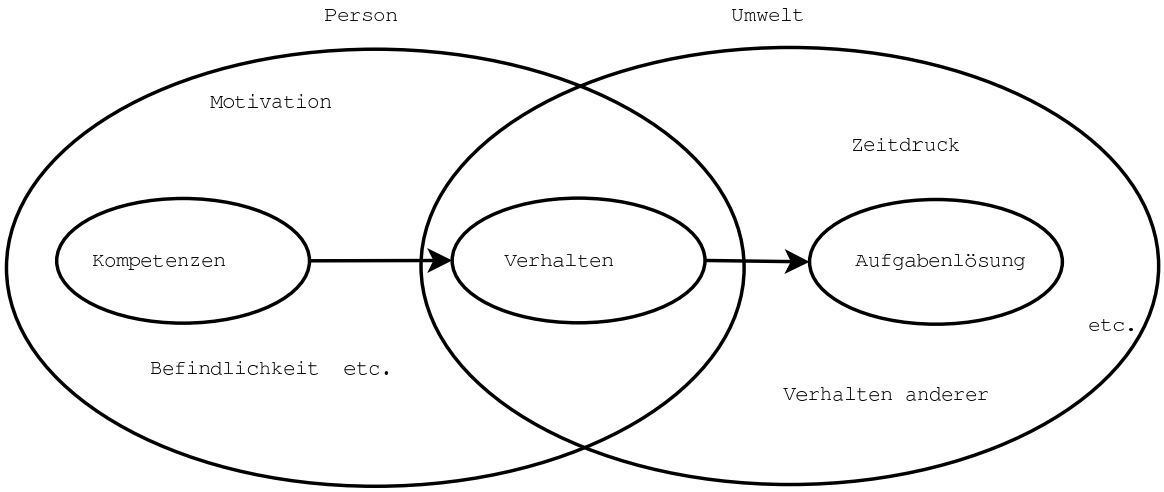

Abbildung 3: Zusammenhang zwischen Kompetenz und Verhalten, selbst erstellt nach Kanning (2007, S. 15)

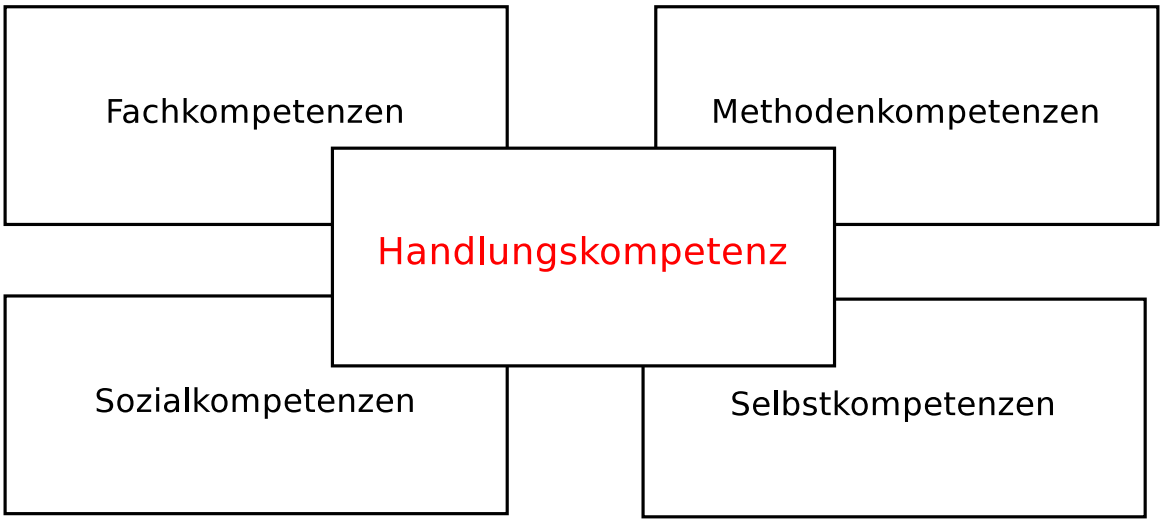

Abbildung 4: Grafische Darstellung der Kompetenzklassen, selbst erstellt

geheimhält und es auf Nachfragen ihrer Bürokollegen oder eines Systemadministrators nicht preisgibt. Da auch hier die Sicherheitsrichtlinie die konkrete Handlung vorschreibt, muss Alice diese Handlung »nur« noch korrekt umsetzen.

Anders verhält es sich im Falle eines mehrdimensionalen verteilten Angriffs, also einer Social-Engineering-Attacke um technische Informationen zu erbeuten, mit denen technische Angriffe gefahren werden können. In der Regel sind professionelle Angriffe strategisch angelegt. Sie verbinden die technische mit der sozialen Dimension, dauern über einen längeren Zeitraumen und bestehen aus mehreren »Scharmützeln« und »Gefechten« auf operativer und taktischer Ebene (von Clausewitz 1832). Das heißt, das ein Angreifer nicht nur verschiedene Computersysteme angreifen wird, sondern auch verschiedene Mitarbeiter. So kann er beispielsweise Alice per Telefon anrufen, sich als Systemadministrator ausgeben, der ein technisches Problem behebt, und sie nach ihrer IP-Adresse fragen. Die Information über die IP-Adresse kann er dann beispielsweise in einer weiteren technischen Attacke nutzen. Bezogen auf die Wissenstreppe (Abbildung 2) heißt das, dass Alice bereits auf der Stufe »Information« und »Wissen« scheitert, da sie nicht weiß, was eine IP-Adresse ist und wie sie der Angreifer für seine Zwecke nutzen kann. Sie muss nun selbständig entscheiden, ob sie die Information herausgibt oder nicht.

Die kompetente Handlung ist nun nicht-determiniert. Problematischer ist aber hierbei, das nicht einmal nach Alicens vollendeter Handlung diagnostiziert werden kann, ob diese Handlung sicherheitskompetent war, da der Erfolg des Angriffs nicht nur von Alicens Handlungen abhängt, sondern eben auch von anderen Organisationsmitgliedern, die angegriffen werden.

Satz 1 (determinierte kompetente Handlung) *Ist das Ergebnis einer kompetenten Handlung bekannt, heiße sie determinierte kompetente Handlung.*

Satz 2 (nicht-determinierte kompetente Handlung) *Ist das Ergebnis einer kompetenten Handlung nicht bekannt, heiße sie nicht-determinierte kompetente Handlung.*

8 Organisationssicherheit

Ich habe bisher gezeigt, dass sich Sicherheit in die technische und psychische Ebene erstreckt. Da Organisationen als soziales System der strukturellen Kopplung von psychischen Systemen bestehen, ist auch die Organisation, also die soziale Dimension zu untersuchen (vgl. Baecker 2005a; Luhmann 2008a; Maturana und Varela 1980; von Foerster 1993c).

Auch wenn man nicht dem Modell des Konstruktivismus und der soziologischen Systemtheorie folgt, werden im Wissensmanagement und der Organisationsentwicklung der Einfluss der Organisation auf die Organisationsangehörigen – und umgekehrt auf vielfältige Weise untersucht (vgl. Brandenburg und Faber 2007; Sonntag 2006; Weber 1947a,b; Witte 1973).

Auch im Falle der IT-Sicherheit gewinnt die Organisation bedeutenden Einfluss: sei es durch ihr formales Organisationsmodell (vgl. Bea und Göbel 2002), der Organisations- und Professionskultur (vgl. Schmid und Messmer 2005), Kommunikationsdynamiken (vgl. Mohr 2006), Lernbarrieren (vgl. Schüppel 1999), Lernkultur (vgl. Willke 2001), die Konstruktion der Wirklichkeit (vgl. Berger und Luckmann 2004) oder schlussendlich der »Vorwegnahme von Entscheidungen« (vgl. Baecker 2005b).

Betrachtet man das Problem der IT-Sicherheit nun aus individueller Sicht wird schnell klar, dass auch die organisationale Sicht nicht ausgeschlossen werden kann. Einerseits natürlich im Rahmen der Personal- und Organisationsentwicklung, andererseits aber auch direkt als Angriffsziel.

Für das erstgenannte Problem möchte ich auf die einschlägige Literatur (vgl. Sonntag 2006) verweisen. Das zweite Problem, dass der Organisation als Angriffsziel, möchte ich im folgenden anhand des historischen Verteidungskonzeptes »Verteidigung in der Tiefe« illustrieren.

9 Verteidigung in der Tiefe

Verteidigung in der Tiefe ist ein Verteidigungskonzept, dass in den mittelalterlichen Städten entstand. Nachdem die Kampfkraft der Artillerie soweit gestiegen war, dass sie Stadtmauern zerstören und so Breschen schlagen konnte, reichten die einfachen Verteidigungsanlagen der Städte nicht mehr aus.

So begann der Festungsbau nicht mehr auf eine starre, aber stark befestigte Stadtmauer als räumlich erzwungene Hauptkampflinie zu setzen, sondern staffelte verschiedene Verteidigungsanlagen in der Tiefe. Diese Verteidigungsanlagen deckten sich gegenseitig durch Waffenwirkung und sperrten die Bewegung des Gegners. Das Konzept war relativ einfach, aber erfolgreich. Verfügte eine Stadt nur über eine einzige Stadtmauer, genügte es für den Angreifer, in diese eine Bresche zu schlagen um die Stadt zu erstürmen.

Im Konzept der Verteidigung in der Tiefe baute man nicht mehr eine einzelne stark befestigte Stadtmauer auf, sondern hintereinander gestaffelt mehrere Mauern und Vorposten, die in der Regel »Vorwerk« genannt wurden. Der Angreifer musste erst die Vorwerke bzw. die ersten Sperren überwinden. Während er dies versuchte, konnten ihn die Verteidiger von den dahinterliegenden Sperren relativ gut geschützt bekämpfen. Der schweren Artillerie des Angreifers konnte es zwar gelingen Breschen zu schlagen, diese führten aber nicht mehr direkt in die Stadt, sondern endeten an der nächsten Sperre, von der aus die Angreifer bekämpft wurden (vgl. Secrétariat général de la défense nationale 2004; Zinsmeister 2009).

Abb. 5 zeigt die Festung Magdeburg um 1750. Die »Zacken« um die Stadmauer Richtung Norden stellen die Vorwerke dar. Ebenso werden die gestaffelten Verteidigungslinien gezeigt. Im Süden der Stadt liegt das Schanzwerk »Turmschanze« als vorgeschobenes

Verteidigungswerk.

Das Konzept wurde in gewisser Weise auch in Pias (2009) diskutiert, vor allem auch in Zinsmeister (2009).

Das Konzept der Verteidigung in der Tiefe wird schon seit einigen Jahren, wenn nicht gar Jahrzehnten, in der IT-Sicherheit angewandt und »gepredigt«[17] (vgl. Secrétariat général de la défense nationale 2004).

Es kann in der technischen Dimension auch vergleichsweise einfach umgesetzt werden, beispielsweise in dem man Netzwerke segmentiert und so voneinander abschottet. Wird ein Laptop der Außendienstler von einem Computervirus verseucht, kann die Firewall hinter dem WLAN-Router dessen Ausbreitung ins Firmennetz stoppen (s. Abb. 6). Es können auch mehrere gestaffelte Sicherheitsmechanismen eingesetzt werden, wie Paketfilter, verschlüsselnde Dateisysteme, Intrusion Detection Systeme und Honeypots, Datensicherung und -vernichtung oder Steuerung der Systemcalls (vgl. Schumacher 2006a,b,c,d, 2007a,b,c,d, 2010).

Die Verteidigung in der Tiefe muss aber nicht nur in der technischen Dimension ausgerollt werden, sondern auch in der sozialen und technisch-sozialen Dimension. Bisher etablierte Beispiele sind die physikalische Sicherung von Computern in speziell geschützten Räumen mit Zugangssbeschränkung oder das Benutzer-Rechte-Konzept auf Mehrbenutzerbetriebssystemen. Dabei bekommt jeder Benutzer ein eigenes Login und Passwort und verschiedene Zugriffsrechte auf Dateien. Erbeutet ein Angreifer das Passwort von Alice kann er zwar Alicens Dateien manipulieren, aber nicht die von Bob.

In der sozialen und technisch-sozialen Dimension lässt sich das Konzept nicht, oder nur unzureichend, mit technischen Mitteln umsetzen. Hier liegt die Verteidigungsaufgabe in Händen der Mitarbeiter, also in deren Entscheidungen. Alice und Bob werden so zum »Vorwerk«, dass die Benutzerpasswörter vor Angreifern schützen muss. Diese »Vorwerk«-Funktion können sie durch eine sicherheitskompetente Handlung wahrnehmen. Dazu sind für beide Kompetenzentwicklungsmaßnahmen notwendig, die sie zur Sicherheitskompetenz befähigen. Neben der individuellen Ebene ist aber auch die organisationale Ebene von Bedeutung. Die Organisation trifft bestimmte Entscheidungen für ihre Angehörigen, ebenso bringt sie ihre Angehörigen dazu, Entscheidungen wahrscheinlich auf eine bestimmte Art zu fällen. Auch wenn eine Bank bestimmte Frisuren ihren Mitarbeitern nicht explizit vorschreibt, gibt es solche die akzeptiert werden und solche die nicht akzeptiert werden. Die »Kultur« der Bank beeinflusst[18] hierbei auch die Wahl der Frisur eines Mitarbeiters.

Da die Organisation also die Entscheidungen, die ihre Angehörigen treffen beeinflusst, hat sie so auch Einfluss auf die Sicherheit der Organisation. Die Soldaten, die der Schuhmacher Voigt als Hauptmann von Köpenick unter sein Kommando gestellt hat, hätten auch dessen Dienstausweis verlangen können. Dies taten sie aber nicht, vermutlich weil sie als Mannschaften einem Offizier gegenüber zu gehorchen hatten. Aber selbst der Bürgermeister von Köpenick überprüfte nicht dessen Authentizität und Autorität. Soll die Sicherheit nun die gesamte Organisation, was zwingend notwendig ist, muss auch das Verhalten der Organisation selbst untersucht und gegebenenfalls zu sicherheitskompetenten Verhalten hin verändert werden. Ich adaptiere hierfür den aus der Biologie (Walker und Salt 2006) und Entwicklungspsychologie (vgl. Brooks und Goldstein 2007) bekannten Begriff der *Resilienz*. Resilienz bedeutet wörtlich zurückspringen und bezeichnet in der Biologie und Psychologie die Widerstandsfähigkeit eines Systems gegenüber äußeren Störungen. Die Entwicklungspsychologie untersuchte beispielsweise die Resilienz und Bildungserfolge von Migranten (vgl. Haines 1989), armen Familien (vgl. Bundeskonferenz für Erziehungsberatung e.V. 2004) oder traumatisierten Adoptivkindern (vgl. Thränhardt und Hunger 2000).

Ich möchte daher dieses Konzept, das auch eng mit der Idee der Lernenden Organisation verwandt ist (vgl. Senge und Klostermann 2008), wie folgt definieren:

Satz 3 (Organisationssicherheit)
Organisationssicherheit bezeichnet die Sicherheit einer Organisation auf technischer, sozialer und technisch-sozialer Ebene. Organisationssicherheit umfasst damit alle Dimensionen der Sicherheit.

Sicherheit muss hiermit nun auch auf der organisationalen Ebene untersucht werden. Dazu möchte ich den Begriff der »Resilienten Organisation« einführen und skizieren:

Satz 4 (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.*

Erst auf organisationaler Ebene ist es also möglich, auf alle möglichen, auch unbekannten, Angriffe zu reagieren. Nur die Organisation kann Fehler in der technischen oder psychischen Dimension erkennen und ausgleichend auf sie reagieren. Sie muss auch in der Lage sein, selbständig neuartige Angriffsmethoden zu identifizeren und selbständig neuartige Abwehrmethoden zu etablieren[19]. Daher ist es im weiteren notwendig, Erkenntnisfähigkeit als Grundlage einer Lernenden Organisation zu untersuchen und Personal- und Organisationskonzepte zu entwerfen, die in Anlehnung an Scharmer (2007); Senge und Klostermann (2008) zu Erkenntnisfähigkeit und selbständigem Handeln auf allen Ebenen führen.

17 http://cryptome.org/0003/nsf020711.pdf v. 2011-02-08

18 Wobei hierbei nicht ganz klar ist ob die Bank die Mitarbeiter formt oder die Mitarbeiter die Bank formen. Die Frage nach der Kausalität wäre in diesem Beispiel aber zu weit gegriffen.

19 Die Diagnostik von Sicherheitsvorfällen und die dazu notwendige Erkenntnisfähigkeit habe ich in Schumacher (2010) diskutiert.

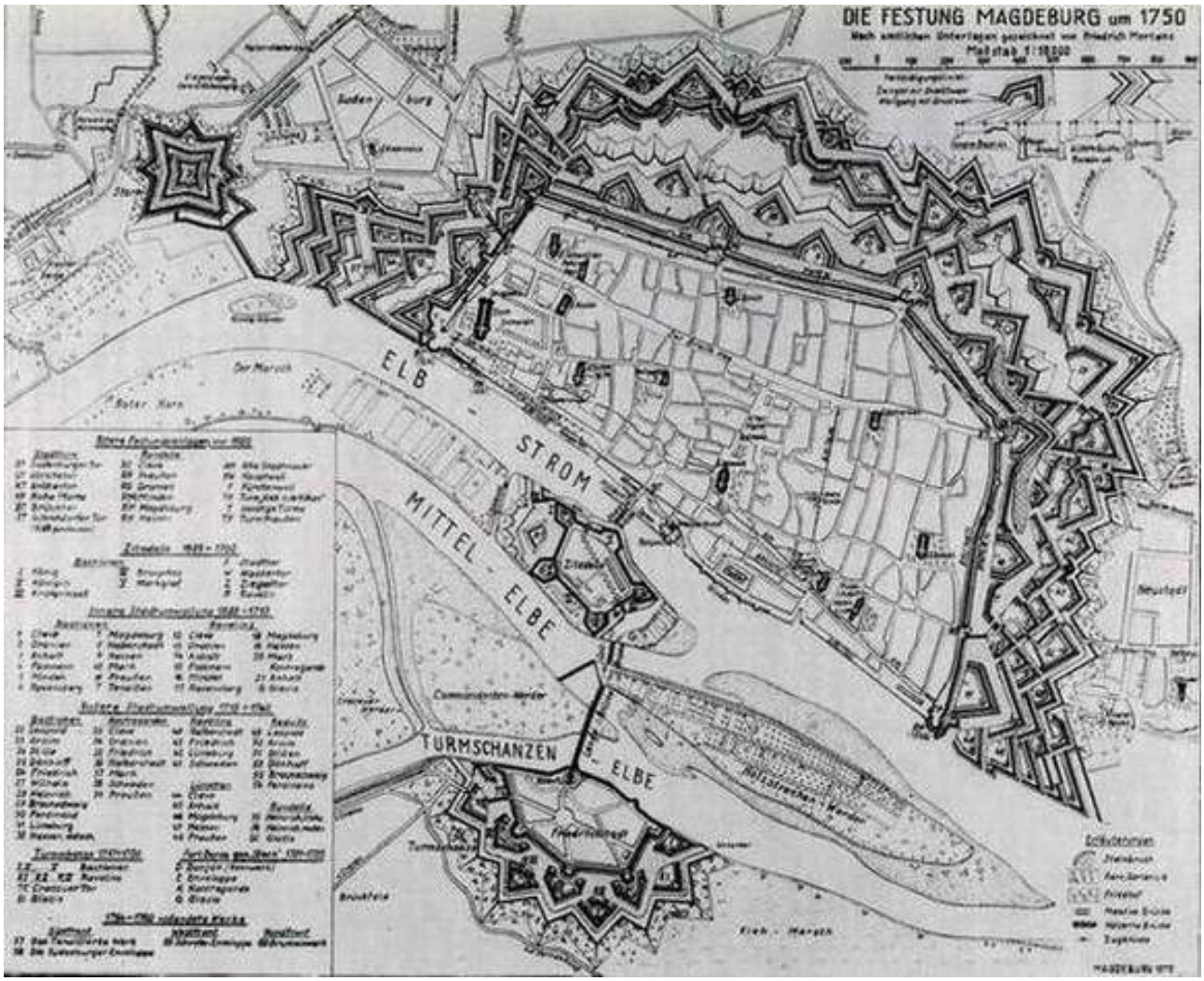

Abbildung 5: Die Festung Magdeburg um 1750

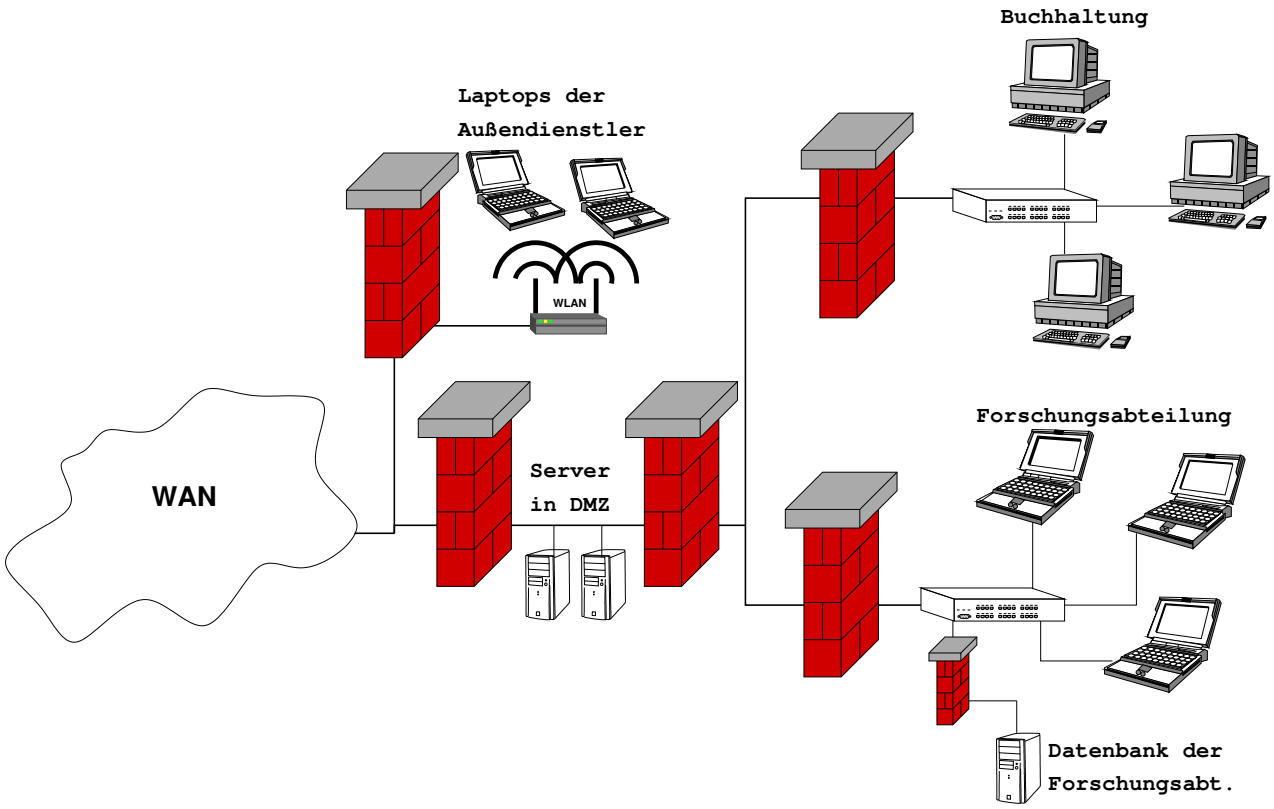

Abbildung 6: Verteidigung in der Tiefe durch Netzsegmentierung mittels Firewalls

Literaturverzeichnis

Aleph One. (1996 November). Smashing The Stack For Fun And Profit. *Phrack*, 7(49). Zugriff 3. Dezember 2006, unter http://www.phrack.com/issues.html?issue=49&id=14

Allen, J., Christie, A. & McHugh, J. (2000 September). Defending Yourself: The Role of Intrusion Detection Systems. Zugriff 4. Januar 2005, unter http://www.cert.org/archive/pdf/IEEE_IDS.pdf

Baecker, D. (Herausgeber). (2005a). *Organisation als System*: Frankfurt: Suhrkamp.

Baecker, D. (2005b). Zum Problem des Wissens in Organisationen. In D. Baecker (Herausgeber), *Organisation als System*: (3. Auflage, Seiten 68–101). Frankfurt: Suhrkamp.

Bea, F. X. & Göbel, E. (2002). *Organisation: Theorie und Gestaltung* (3., neu bearbeitete Auflage). Stuttgart: Lucius und Lucius.

Beck, U. (2007). *Weltrisikogesellschaft: Auf der Suche nach der verlorenen Sicherheit*. Frankfurt: Suhrkamp.

Berger, P. L. & Luckmann, T. (2004). *Die gesellschaftliche Konstruktion der Wirklichkeit: Eine Theorie der Wissenssoziologie* (20. Auflage). Frankfurt: Fischer.

Brandenburg, T. & Faber, T. (2007). Fehlermanagement-Training – Entwicklung sozialer Kompetenzen und der Umgang mit Fehlern in Risiko-Arbeitsbereichen. In U. P. Kanning (Herausgeber), *Förderung sozialer Kompetenzen in der Personalentwicklung* (1. Auflage, Seiten 216–237). Göttingen: Hogrefe.

Brooks, R. & Goldstein, S. (2007). *Das Resilienz-Buch: Wie Eltern ihre Kinder fürs Leben stärken, das Geheimnis der inneren Widerstandskraft*. Stuttgart: Klett-Cotta.

Bundesamt für Sicherheit in der Informationstechnik (Herausgeber). (2006). Leitfaden IT-Sicherheit IT-Grundschutz kompakt. Zugriff 16. Oktober 2006, unter http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

Bundeskonferenz für Erziehungsberatung e.V. (Herausgeber). (2004). Arme Familien gut beraten: Hilfe und Unterstützung für Kinder und Eltern. Zugriff 5. Januar 2011, unter http://www.bke.de/content/application/shop.download/1257417004_Arme%20familien%20PM%2072.pdf

Davidow, W. & Malone, M. (1992). *The virtual corporation: structuring and revitalizing the corporation for the 21st century*. HarperBusiness.

Deutsches Institut für Normung. (2002). DIN EN 61508 / VDE 0803: Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme.

Deutsches Institut für Normung. (2008). DIN EN ISO 13857: Sicherheit von Maschinen - Sicherheitsabstände gegen das Erreichen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen.

Erpenbeck, J. & Sauter, W. (2007). *Kompetenzentwicklung im Netz: New Blended Learning mit Web 2.0* (1. Auflage). Luchterhand (Hermann).

Erpenbeck, J. & von Rosenstiel, L. (Herausgeber). (2007). *Handbuch Kompetenzmessung: Erkennen, verstehen und bewerten von Kompetenzen in der betrieblichen, pädagogischen und psychologischen Praxis* (2., überarb. und erw. Aufl.). Stuttgart: Schäffer-Poeschel.

Gessler, M. (2006). Das Kompetenzmodell. In R. Bröckermann & M. Müller-Vorbrüggen (Herausgeber), *Handbuch Personalentwicklung – Die Praxis der Personalbildung, Personalförderung und Arbeitsstrukturierung* (1. Ausgabe, Seiten 23–42). Stuttgart: Schäffer-Poeschel Verlag.

Hacker, W. (2005). *Allgemeine Arbeitspsychologie* (2., vollst. überarb. u. erg. A.). Göttingen: Verlag Hans Huber.

Haines, D. W. (Herausgeber). (1989). *Refugees as Immigrants: Cambodians, Laotians and Vietnamese in America* (1. Auflage). Totowa: Rowman und Littlefield.

Kanning, U. P. (2007). Soziale Kompetenzen in der Personalentwicklung. In U. P. Kanning (Herausgeber), *Förderung sozialer Kompetenzen in der Personalentwicklung* (1. Auflage, Seiten 12–38). Göttingen: Hogrefe.

Kauffeld, S., Grote, S. & Frieling, E. (2003). Das Kasseler-Kompetenz-Raster (KKR). In J. Erpenbeck & L. von Rosenstiel (Herausgeber), *Handbuch Kompetenzmessung* (Seiten 261–281). Stuttgart: Schäffer-Poeschel.

Kompetenzraster im Mathematikunterricht der Grundschule. (2007). Zugriff 22. April 2009, unter http://bildungsserver.berlin-brandenburg.de/fileadmin/bbb/unterricht/faecher/naturwissenschaften/mathematik/Begleitheft_Kompetenzraster.pdf

Langens, T. A., Sokolowski, K. & Schmalt, H.-D. (2003). Das Multi-Motiv-Gitter (MMG). In J. Erpenbeck & L. von Rosenstiel (Herausgeber), *Handbuch Kompetenzmessung* (Seiten 71–79). Stuttgart: Schäffer-Poeschel.

Lemken, B. & Cremers, A. B. (1999). Virtuelle Organisationen: organisatorische und technische Aspekte. In *Tagungsband zum Workshop des Forschungsverbundes NRW Multimedia und Gesellschaft*. Zugriff 25. Oktober 2008, unter http://www.cs.uni-bonn.de/~prosec/virto/WorkshopBadHonnef99.pdf

Luhmann, N. (1999). *Zweckbegriff und Systemrationalität* (11. Auflage). Frankfurt: Suhrkamp.

Luhmann, N. (2008a). *Einführung in die Systemtheorie* (4. Auflage) (D. Baecker, Herausgeber). Heidelberg: Carl-Auer Verlag.

Luhmann, N. (2008b). *Legitimation durch Verfahren* (12. Auflage). Frankfurt: Suhrkamp.

Maturana, H. & Varela, F. (1980). *Autopoiesis and Cognition: The Realization of the Living* (1. Auflage). Dordrecht (NL): D. Reidel.

Mertens, D. (1974). Schlüsselqualifikationen: Thesen zur Schulung für eine moderne Gesellschaft. *Mitteilungen aus der Arbeitsmarkt- und Berufsforschung*, *7*, 36–43. Zugriff 22. Mai 2009, unter http://doku.iab.de/mittab/1974/1974_1_MittAB_Mertens.pdf

Mohr, G. (2006). *Systemische Organisationsanalyse: Dynamiken und Grundlagen der Organisationsentwicklung*. Bergisch Gladbach: EHP.

Nonaka, I. & Takeuchi, H. (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* (1. Aufl.). Oxford: Oxford University Press.

North, K. (2002). *Wissensorientierte Unternehmensführung: Wertschöpfung durch Wissen* (2., aktualisierte und erw. Aufl.). Wiesbaden: Gabler.

Pias, C. (Herausgeber). (2009). *Abwehr*: *Modelle Strategien Medien* (1. Auflage). Bielefeld: transcript.

Poser, H. (2001). *Wissenschaftstheorie* (1. Auflage). Stuttgart: Reclam.

Raymond, E. S. (1999). *The Cathedral and the Bazaar* (1st) (T. O'Reilly, Herausgeber). Sebastopol, CA, USA: O'Reilly & Associates, Inc.

Scharmer, C. O. (2007). *Theory U: Leading from the Future as it Emerges*. Cambridge: The Society for Organizational Learning.

Schmid, B. & Messmer, A. (2005). *Systemische Personal-, Organisations- und Kulturentwicklung: Konzepte und Perspektiven*. Bergisch Gladbach: EHP.

Schumacher, S. (2006a). Methoden zur Datensicherung – Strategien und Techniken für NetBSD. net-tex.de. Zugriff unter http://www.net-tex.de/backup.pdf

Schumacher, S. (2006b). Methoden zur Datensicherung – Strategien und Techniken für NetBSD. In German Unix User Group (Herausgeber), *Proceedings des GUUG Frühjahrsfachgespräches 2006*, (Seiten 79–98). Universität Osnabrück. Berlin: Lehmanns Media.

Schumacher, S. (2006c). Sicherung verteilter Systeme mit Bacula. *UpTimes*, *4*, 14–20. Zugriff 7. November 2009, unter http://kaishakunin.com/publ/guug-uptimes-bacula.pdf

Schumacher, S. (2006d). Verschlüsselte Dateisysteme für NetBSD. *UpTimes*, *4*, 25–31. Zugriff 7. November 2009, unter http://kaishakunin.com/publ/guug-uptimes-cgd_cfs.pdf

Schumacher, S. (2007a). Daten sicher löschen. *UpTimes*, *1*, 7–16. Zugriff 7. November 2009, unter http://kaishakunin.com/publ/guug-uptimes-loeschen.pdf

Schumacher, S. (2007b). PostgreSQLs Datenbestände sichern. *UpTimes*, *2*, 4–7. Zugriff 7. November 2009, unter http://kaishakunin.com/publ/guug-uptimes-postgresql.pdf

Schumacher, S. (2007c). Systemaufrufe mit Systrace steuern. *UpTimes*, *4*, 12–19. Zugriff 7. November 2009, unter http://kaishakunin.com/publ/guug-uptimes-systrace.pdf

Schumacher, S. (2007d). Systeme mit Systrace härten. *Die Datenschleuder: Das wissenschaftliche Fachblatt für den Datenreisenden*, *#91*, 40–48. Zugriff 3. Januar 2008, unter http://ds.ccc.de/pdfs/ds091.pdf

Schumacher, S. (2008). Soziale Kompetenzen für Informatiker. Unveröffentlichte Hausarbeit im Fach »Stellenwert von Kompetenzdiagnostik innerhalb der Kompetenzentwicklung«. Otto-von-Guericke-Universität Magdeburg.

Schumacher, S. (2010). Auf dem Weg zum Intrusion Detection System der nächsten Generation. In Team der Chemnitzer Linux-Tage (Herausgeber), *Chemnitzer Linux-Tage 2010: Tagungsband*, (Seiten 19–24). Technische Universität Chemnitz. Chemnitz: Universitätsverlag.

Schumacher, S. (2013). Vom Cyber-Frieden. *Magdeburger Journal zur Sicherheitsforschung*, *1*, 354–369. Zugriff 15. März 2013, unter http : / / www . sicherheitsforschung - magdeburg . de / publikationen.html

Schüppel, J. (1999). *Wissensmanagement: Organisatorisches Lernen im Spannungsfeld von Wissens- und Lernbarrieren* (1. Auflage). Wiesbaden: Deutscher Universitätsverlag.

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. (2007). Zugriff 22. April 2009, unter http : / / www . kmk . org / fileadmin / veroeffentlichungen_beschluesse / 2007 / 2007_09_01-Handreich-Rlpl-Berufsschule.pdf

Senge, P. & Klostermann, M. (2008). *Die fünfte Disziplin: Kunst und Praxis der lernenden Organisation*. Schäffer-Poeschel Verlag.

Sonntag, K. (Herausgeber). (2006). *Personalentwicklung in Organisationen*. Bern: Hogrefe.

Staudt, E., Kailer, N. & Kottmann, M. (2002). *Kompetenzentwicklung und Innovation* (1. Auflage). Münster: Waxmann.

Thränhardt, D. & Hunger, U. (2000). *Einwanderer-Netzwerke und ihre Integrationsqualität in Deutschland und Israel*. Studies in migration and minorities. Lit.

Secrétariat général de la défense nationale (Herausgeber). (2004). Die Verteidigung in der Tiefe angewandt auf IT-Systeme (Memento). Zugriff 25. Oktober 2006, unter http: / / www.ssi.gouv.fr / de / vertrauen / documents / methods / mementodep-V1.1_de.pdf

von Clausewitz, C. (1832). *Vom Kriege*. Ferdinand Dümmler.

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

von Foerster, H. (1993b). Die Verantwortung des Experten. In S. J. Schmidt (Herausgeber), *Wissen und Gewissen: Versuch einer Brücke*: (1. Auflage, Seiten 337–346). Frankfurt: Suhrkamp.

von Foerster, H. (1993c). Über selbst-organisierende Systeme und ihre Umwelten. In S. J. Schmidt (Herausgeber), *Wissen und Gewissen: Versuch einer Brücke*: (1. Auflage, Seiten 211–232). Frankfurt: Suhrkamp.

von Foerster, H. (2008). Ethik und Kybernetik zweiter Ordnung. In P. Watzlawick & G. Nardone (Herausgeber), *Kurzzeittherapie und Wirklichkeit* (Seiten 71–89). München: Piper.

Walker, B. & Salt, D. (2006). *Resilience thinking: sustaining ecosystems and people in a changing world*. Island Press.

Weber, M. (1947a). Wirtschaft und Gesellschaft. In *Grundriss der Sozialökonomik* (3te Auflage, Band 1). Tübingen: P. Siebeck. Zugriff 13. April 2008, unter http: / / gallica2.bnf.fr / ark: /12148 / bpt6k94382s.download

Weber, M. (1947b). Wirtschaft und Gesellschaft. In *Grundriss der Sozialökonomik* (3te Auflage, Band 2). Tübingen: P. Siebeck. Zugriff 13. April 2008, unter http: / / gallica2.bnf.fr / ark: /12148 / bpt6k943834.download

Willke, H. (2001). *Systemisches Wissensmanagement* (2., neubearb. A.). Stuttgart.

Witte, E. (1973). *Organisation für Innovationsentscheidungen - Das Promotoren-Modell* (1. Auflage). Göttingen: Schwartz.

Zinsmeister, A. (2009). Abwehr: Urbane Topographien. In C. Pias (Herausgeber), *Abwehr*: *Modelle Strategien Medien* (1. Auflage, Seiten 147–168). Bielefeld: transcript.