SICHERHEIT MESSEN. EINE OPERATIONALISIERUNG ALS LATENTES SOZIALES KONSTRUKT

Stefan Schumacher

1 Einführung und Motivation

Im Zuge der informationstechnologischen Revolution der letzten 40 Jahre hielten und halten Computer in verschiedensten Formen Einzug in nahezu alle Lebensbereiche. Angefangen hat diese Entwicklung mit den ersten größeren Einsätzen im Militär (Enigma und Turing-Bombe) zu Beginn des Zweiten Weltkrieges und dem Einzug in die zuerst militärische Forschung (ENIAC und Arpanet) des daraus folgenden Kalten Krieges. In den 1950er bis 1970er Jahren eroberten die Großrechner auch die zivile Forschung und über die Betriebswirtschaftslehre ihren Platz in großen Unternehmen. Im Zuge der Entwicklung der Integrierten Schaltkreise wurden Computer immer leistungsfähiger und immer kleiner, bis sie in Gestalt des 1981 vorgestellten IBM PCs auch die Schreibtische und später die Wohn- und Kinderzimmer eroberten. Ein weiterer Meilenstein war die Ausbreitung des Internets in Deutschland ab Mitte der 1990er Jahre und anschließend die Entwicklung des von William Gibson bereits in den 1980er prophezeiten Cyberspace als „computermedial erzeugte[m] Sinnhorizont“[1].
Mit dem Ende der ersten Dekade des 21. Jahrhunderts traten leistungsfähige Smartphones ihren Siegeszug an und führten in Verbindung mit sozialen Netzwerken zur ersten Generation von sog. Digital Natives[2], also Kindern und Jugendlichen die mit und im Netz aufgewachsen sind.
Weder aus den Unternehmen noch aus den Haushalten sind Computer und Internet wegzudenken. So nutzen nach einer Statistik[3] des Branchenverbandes BITKOM bereits mehr als drei Viertel aller deutschen Haushalte einen Internetzugang, wobei zwei Drittel aller Haushalte Breitbandinternet und jeder vierte Deutsche mobile Internetzugänge via Laptop oder Handy nutzen. Ebenso nutzen in Deutschland 61 % aller Beschäftigten einen Computer am Arbeitsplatz. Es ist also heute schon fast unnormal geworden keinen Computer zu benutzen, zumindest wenn man zu den Jugendlichen oder Erwerbstätigen gehört.
Im Rahmen der Verbreitung von Computern, IT und Internetzugängen wurden und werden immer mehr Tätigkeiten und Angebote via Internet angeboten. Seien es soziale Netzwerke wie Facebook, StudiVZ oder Xing, die ohne PCs und Internet gar nicht möglich wären oder Business-2-Comsumer-Angebote (B2C) wie Internetbanking oder Handelsplattformen à la Ebay und Amazon. Auch in der Wirtschaftswelt sind vie-

1 http://de.wikipedia.org/w/index.php?title=Cyberspace&oldid=85161862 v. 2011-03-03

2 http://www.sueddeutsche.de/kultur/born-digital-nicht-ohne-mein-offline-selbst-1.531588 v. 2011-03-03

3 http://www.bitkom.org/de/markt_statistik/64003.aspx v. 2011-03-03

le Dienste nur noch via Internet verfügbar, zum Beispiel die sogenannten Business-2-Business-Dienste (B2B) wie die weltweite Kooperation von Softwareentwicklern oder der Datenaustausch zwischen Automobilherstellern und Zulieferern, der fast ausnahmslos virtuell stattfindet. Auch Produktionsanlagen[4] und Geräte kommunizieren inzwischen immer mehr über das Internet miteinander, so sollen beispielsweise nach dem Willen der EU sogenannte Smart Meter[5], also „intelligente" Stromzähler eingeführt werden, die den Verbrauch der Haushalte direkt und in Echtzeit an die Stadtwerke und Kraftwerke melden. Die Stromerzeuger sind auch interessiert daran, den Jahresverbrauch online auszulesen, um die Kosten für menschliche Ableser einzusparen. Außerdem sollen aus Kostengründen die Smart Meter per Remote-Zugang abschaltbar sein, damit im Falle des Zahlungsverzugs oder Auszugs eines Kunden der Stromzugang sofort und bequem gekappt werden kann. All diese Szenarien bergen jedoch ein entscheidendes Problem, das der Sicherheit.

Neben „einfachen" Sicherheitsproblemen, wie den verbreiteten Viren, Würmern und Trojanern sowie Spam- und Phishing-Mails, gibt es tagtäglich wenig elaborierte aber automatisierbare Angriffe gegen Internetbanking, die zwar eine geringe Erfolgsquote haben, in der Masse aber zu erklecklichen Gewinnen bzw. Schäden führen. Abbildung 1.1 zeigt die beim CERT Coordination Center der Carnegie Mellon University katalogisierten Sicherheitslücken in Software. Sie stiegen von 171 im Jahre 1995 auf 7236 im Jahre 2007. Abbildung 1.2 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 weiterer zurzeit heiß diskutierter Punkt ist der des Datenschutzes im Netz, die sogenannte Privacy-Debatte. So stellen beispielsweise viele Jugendliche sorgenlos Informationen und unvorteilhafte Fotos in sozialen Netzwerken ein, ohne sich bewusst zu sein, dass diese automatisiert analysiert werden und im späteren Leben durchaus problematisch sein können.

In der Wirtschaft spielt die IT-Sicherheit inzwischen auch eine große Rolle. Seien es Vorgänge wie Wirtschaftsspionage[6] oder Sabotage durch verärgerte Mitarbeiter. Auch Sicherheitsfehler in technischen Anlagen können zum Beispiel in Kernkraftwerken, Flugzeugen oder in der Raumfahrt[7] zu massiven, mitunter tödlichen, Konsequenzen

4 http://www.heise.de/security/meldung/Stuxnet-Wurm-kann-Industrieanlagen-steuern-1080584.html v. 2011-03-03

5 http://www.heise.de/security/meldung/Intelligente-Stromzaehler-Entwurf-fuer-Schutzprofil-zur-Diskussion-gestellt-1180901.html v. 2011-03-03

6 http://www.heise.de/newsticker/meldung/Verfassungsschutz-registriert-zunehmende-Wirtschaftsspionage-uebers-Internet-219591.html v. 2011-03-03

7 http://en.wikipedia.org/w/index.php?title=Death_by_PowerPoint&oldid=415751189 v. 2011-03-03

führen. Ebenso werden in der Politik und dem Militär seit einiger Zeit technische Sicherheitsprobleme antizipiert. So ist es theoretisch möglich über Sicherheitslücken[8] in den geplanten Smart Metern in einer konzertierten Aktion alle angeschlossenen Haushalte aus dem Stromnetz herauszuschießen. Dies würde in der Folge aufgrund auftretender Überlastung der Stromnetze zum kaskadierenden Ausfall der Stromerzeuger führen. Da die Kraftwerke europaweit im Europäischen Verbundnetz zusammengeschlossen sind, könnten die Ausfälle kaskadieren und im Endeffekt die Stromversorgung in allen angeschlossenen Ländern ausschalten. Das heißt, dass ein einziger Implementierungsfehler in den Smart Metern halb Europa über Nacht in das „finstere Mittelalter der Stromlosigkeit" zurückkatapultieren könnte.

Gegenwärtig läuft daher, getrieben von Stuxnet[9] und diversen Spionagevorfällen10, eine internationale Cyberwar-Debatte, in der viele Akteure von einem Krieg im Cyberspace ausgehen. Es wird also zurzeit nach Beck[11] ein Weltzustand antizipiert, den es (noch) nicht gäbe. Dies führe dazu, dass im Rahmen der „Weltrisikogesellschaft" eine politische Kraft entstünde, die die Welt verändere. So stellen inzwischen diverse Staaten Cyberwar-Truppen oder Kommandos auf und es werden strategische Szenarien entwickelt, in denen Dritte-Welt-Staaten wie Nord-Korea oder Pakistan führende militärische Weltmächte wie die USA erfolgreich im Cyberspace „bekriegen".

Es zeigt sich also, dass der Einsatz von Informationstechnologie nicht nur Vorteile bietet, sondern insbesondere im Bereich der Sicherheit noch viele Probleme bestehen.

Zwar gibt es in der Informatik seit diversen Sicherheitsvorfällen in den 1970er und 1980er Jahren[12] eine angeregte Diskussion um Sicherheitslücken und -vorfälle. Allerdings wird diese in der Regel eher vom technisch-ingenieurwissenschaftlichen Standpunkt aus geführt. So befassen sich beispielsweise viele Hacker-Konferenzen mit der durchaus notwendigen Diskussion oder Vorstellung der aktuellsten Sicherheitslücken, allerdings werden hierbei die Anwender, also die Menschen, recht häufig ausgeblendet oder eher unwissenschaftlich behandelt.

Im Laufe der letzten mehr als 17 Jahre, in denen ich mich mit IT-Sicherheit als Laie, Nerd, Hacker, Open-Source-Entwickler, Informatik-Student, Systemadministrator, Unternehmensberater, Dozent und Trainer, Sicherheitsforscher und schlussendlich Student der Bildungswissenschaft und Psychologie befasst habe, sind mir diverse Probleme in der allgemeinen Diskussion der IT-Sicherheit aufgefallen.

So gibt es zwar in der Informatik als Ingenieurwissenschaft eine angeregte Diskussion technischer Sicherheitsprobleme, die zu einer starken Professionalisierung der technischen Sicherheitsanalysen und auch Forschung geführt hat. Allerdings fehlen

8 Siehe dazu auch die Berichte und Interviews zu meinem Vortrag „Cyberwar on the Horizon" auf der DeepSec 2010 unter http://fm4.orf.at/stories/1668976/ v. 29.11.2010, http://www.dradio.de/dlf/sendungen/computer/1329500/ v. 29.11.2010, https://www.gulli.com/news/deepsec-2010-der-cyber-war-aus-politischer-sicht-2010-11-28 v. 29.11.2010

9 http://www.heise.de/thema/Stuxnet v. 2011-03-03

10 http://www.spiegel.de/politik/ausland/0,1518,502118,00.html v. 2011-03-03

11 U. Beck. Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit. 2007, S. 29 .

12 vgl. u. a. K. Thompson. „Reflections on Trusting Trust". In: Communications of the ACM 27.8 (Aug. 1984), S. 761–763; C. Stoll. Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten. 1991.

eine grundlegende Diskussion des Sicherheitsbegriffes und dessen Anwendbarkeit. Die Informatik nimmt in der Tradition der Mathematik stehend zwar Definitionen vor, diskutiert diese in der Regel aber nicht, wie es beispielsweise die Pädagogik oder Psychologie tun würde.
So sind in der IT-Sicherheitsszene sogenannte Security-Awareness-Kampagnen äußerst beliebt. Auch ich führe derartige Maßnahmen als Unternehmensberater durch und verdiene damit meinen Lebensunterhalt, außerdem habe ich mich im Rahmen des Studiums mit diesen Maßnahmen bereits praktisch auseinandergesetzt[13].

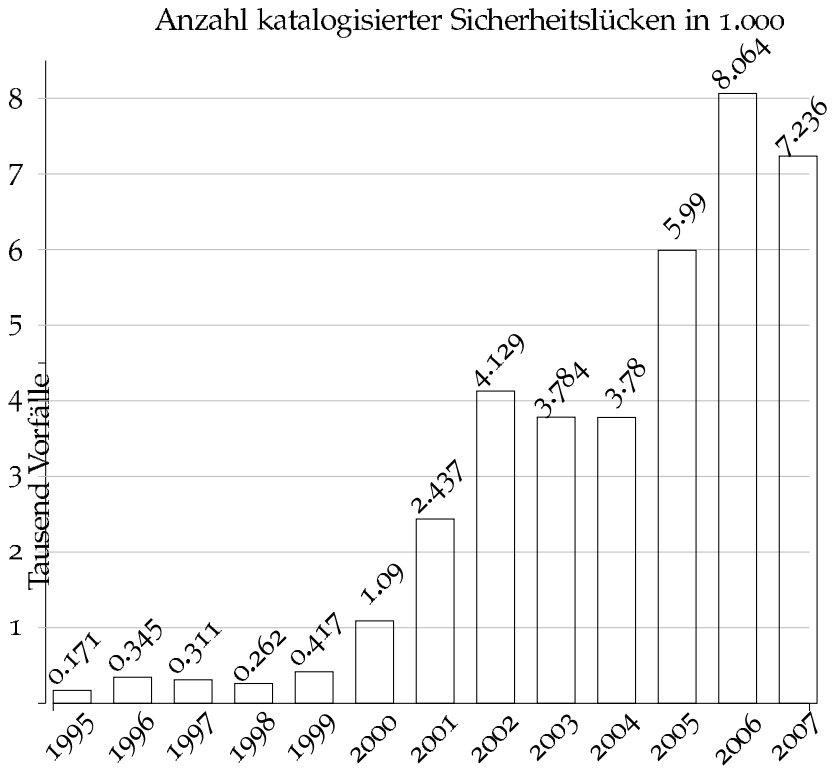


Abbildung 1.1: Beim CERT/CC katalogisierte Sicherheitslücken

Es gibt zwar verschiedene Empfehlungen und Dokumente[14] zur Gestaltung solcher Kampagnen, die sich auch mit der menschlichen Komponente befassen, diese haben in der Regel aber eher Handbuchcharakter und sind selten wissenschaftlich fundiert.

13 vgl. S. Schumacher und J. N. Wilcke. Design und Implementierung einer Security-Awareness-Kampagne. Otto-von-Guericke-Universität Magdeburg, 2008; S. Schumacher. Moderne Mitarbeiterführung. Lernmotivation, Feedback, Evaluation und Qualitätsmanagement in der Weiterbildung. Otto-von-Guericke-Universität Magdeburg, 2010.

14 M. Wilson, D. E. de Zafra, S. I. Pitcher, J. D. Tressler und J. B. Ippolito. Information Technology Security Training Requirements: A Role- and Performance-Based Model. 2003; M. Wilson und J. Hash. Building an Information Technology Security Awareness and Training Program. 2003.

So fehlen in den beiden genannten Dokumenten fundierte Hinweise zur Didaktik, Lerntheorien und Lernmethoden ebenso wie adäquate Evaluationsmethoden, die aber zwingend erforderlich sind, um Personalentwicklungsmaßnahmen professionell durchzuführen[15].

Das in Abbildung 1.3 gezeigte Modell der „Awareness Training Education Schichtung" aus der Abhandlung von Wilson und Hash[16], legt hier aber eher Wert auf funktionale Rollen, („Bürokratie") statt kompetente Handlung. So kommt im gesamten Dokument der Begriff Motivation auch nur genau einmal auf Seite 39 vor: „Motivation demonstrated by those playing key roles in managing/coordinating the security program" sei ein Erfolgsindikator.

Meiner Meinung nach ist das aus pädagogisch/psychologischer Sicht absolut nicht ausreichend. Trotz vereinzelter Kooperation mit anderen Wissenschaften wie Pädagogik, Psychologie und Soziologie gibt es bisher noch keinen geeigneten theoretischen Rahmen, der das individuelle Erleben und Verhalten einzelner Individuen im Umgang mit Informationstechnologie und in Bezug auf die IT-Sicherheit beschreibt. Des Weiteren fehlt die Erweiterung des individuellen Verhaltens einzelner Anwender hin zum organisationalen Verhalten in Gruppen bzw. Organisationen.

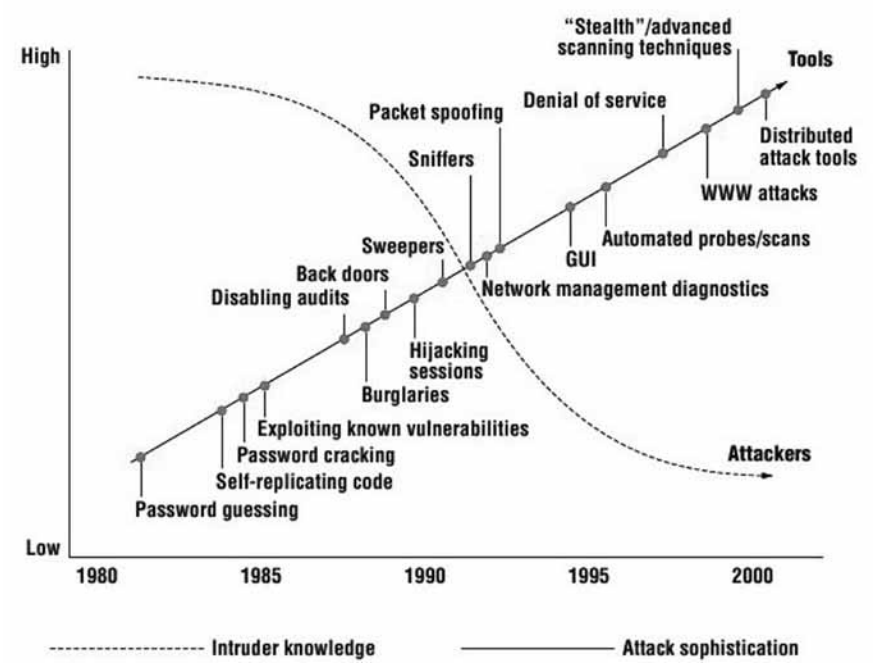


Abbildung 1.2: Angriffs-Komplexität und Angreiferfertigkeiten

15 vgl. J. Reischmann. Weiterbildungs-Evaluation: Lernerfolge messbar machen. 2002.

16 Wilson und Hash, s. Anm. 15, S. 8.

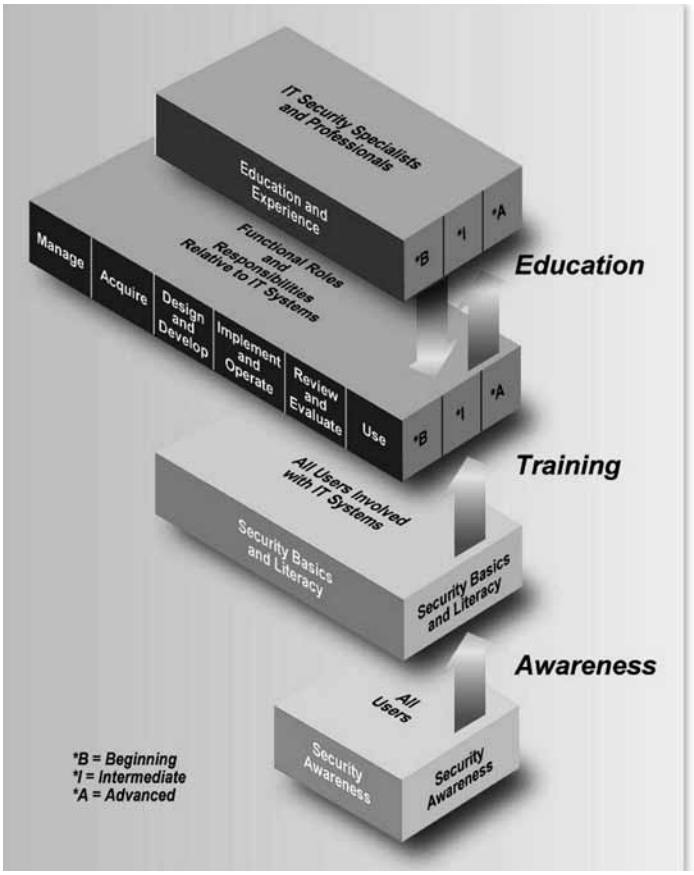


Abbildung 1.3: The IT Security Learning Continuum.

Es mangelt meiner Meinung nach an einer Theorie, die die drei Ebenen Informationstechnologie ↔ Individuum ↔ Organisation umfassend bezüglich der Prognose, Diagnose und Intervention von IT-Sicherheit miteinander verknüpft. Ziel dieser Theorie soll es sein, meine Tätigkeit als Berater für Organisationssicherheit zu professionalisieren, indem geeignete Konstrukte der Sicherheit und darauf aufbauende Werkzeuge zur Messung dieser Konstrukte entwickelt werden.
Diese Konstrukte sowie ihre Methoden und Werkzeuge sollen den grundlegenden Rahmen für eine weitere Professionalisierung der Sicherheitsforschung und vor allem Beratung/Entwicklung legen, beispielsweise für eine Didaktik der Sicherheit oder geeignete Kompetenzmodelle sowie notwendige Fähigkeiten, Fertigkeiten und Kenntnisse.
Weiterhin sollen die Konstrukte als Grundlage für eine professionalisierte Beratung dienen, die neben der technischen auch psychologische und soziologische Dimensionen berücksichtigt. Dies ist notwendig, um Sicherheitsberatungsmaßnahmen wie Schulungen, Trainings und Sensibilisierungen in eine umfassende Sicherheitsstrategie einzubinden. Ich möchte also wissenschaftlich fundierte Diagnose-, Prognose- und

Interventionsmethoden für die Sicherheit von IT-Systemen entwickeln. Dazu ist es zuerst notwendig, den Begriff Sicherheit zu explizieren und die Messbarkeit des Konstruktes zu untersuchen.

Meine zentrale Hypothese lautet daher:

> 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.

Dazu stelle ich folgende Propositionen auf, die ich im Rahmen dieses Aufsatzes untersuchen werde:

Proposition 1 (Sicherheit als Konstrukt)
Sicherheit ist ein latentes soziales Konstrukt.

Proposition 2 (Berechenbarkeit der Sicherheit)
Sicherheit ist nicht trivial berechenbar. Die Sicherheit eines IT-Systems hängt von nicht-trivialen Entscheidungen ab.

Proposition 3 (Dimensionen der Sicherheit)
Sicherheit beschränkt sich nicht auf technische Systeme sondern erstreckt sich auch auf psychische und soziale Systeme.

Proposition 4 (Diagnose – Prognose – Intervention)
Um die Sicherheit eines IT-Systems zu untersuchen und zu verbessern, werden Werkzeuge und Methoden der Diagnose, Prognose und Intervention benötigt.

Proposition 5 (Methoden der Sicherheitsdiagnostik)
Die Werkzeuge und Methoden der Sicherheits-Diagnose, Sicherheits-Prognose und Sicherheits-Intervention erstrecken sich in technische, psychologische und soziale Systeme.

Ich möchte also klären, inwieweit die bisher verbreiteten technischen Sicherheitsmaßnahmen ausreichen, und ob diese technischen Maßnahmen auch in der psychischen und sozialen Dimension greifen. Desweiteren möchte ich untersuchen, wie Sicherheit in der psychischen und sozialen Dimension beschrieben und verändert werden können.

2 Berechenbarkeit der Sicherheit

2.1 Messen, Ordnen und Berechnen

Dieser Aufsatz diskutiert die Fragen der Messbarkeit der Sicherheit, daher ist es zwangsläufig notwendig, den Begriff des Messens zu untersuchen und eine geeignete Definition oder Explikation vorzulegen. Dies ist unumgänglich, da Diagnose und Intervention vergleichen, also messen, bedeuten. Die Statistik als mathematische Disziplin versucht nach Fröhlichs[17] Hypothesen innerhalb eines Wertebereichs durch Stichprobenerhebung zu prüfen. Dazu verbinde sie die Hypothese mit der Erfahrungswelt.

Wendt[18] beschreibt am Beispiel der statistischen Entscheidungstheorie und Bayes-Statistik nach welchen Entscheidungen Aussagen, also „Sätze in den Kanon des „Wissens" aufgenommen werden sollen und welche nicht". Er führt dazu aus, dass die Psychologie als empirische Wissenschaft nicht nur Beobachtetes beschreiben, sondern auch auf bisher unbeobachtete Fälle generalisieren sowie erklären und vorhersagen will. Dazu verwende die psychologische Statistik unter anderem Skalierungsverfahren, die eine psychologische Variable auf einen Zahlenwert abbilden. Dieser Zahlenwert könne dann genutzt werden, um die Variablen zu operationalisieren und sie z. B. in einer Skala abzutragen.

Süß[19] definiert Messen als „Zuordnung von Zahlen zu Objekten, nach bestimmten Regeln, die gewährleisten, dass die Relationen in der Menge der Objekte in der Menge der Zahlen erhalten bleiben, in beiden Mengen also gleich ist". Dabei entstehe eine strukturerhaltende, homomorphe Abbildung zwischen der Menge von Objekten und deren Relationen (genannt empirisches Relativ) sowie der Menge von Zahlen und deren Relationen (genannt numerisches Relativ). Die homomorphe Abbildung zwischen den Relativen bestimmt das Skalenniveau, also die Operationen, die auf die Zahlen angewendet werden können. Die möglichen Skalenniveaus umfassen die Nominalskala, bei der einem Objekt oder einer Klasse von Objekten ein Wert zugeordnet wird. Beispielsweise 1 für männliche VPn, 2 für weibliche VPn. Nominalskalierte Variablen können nicht geordnet werden. Ordinalskalen ermöglichen die Ordnung auf einer Dimension, wie größer/kleiner oder besser/schlechter. So ist die Schulnote 1 besser als eine 2, 2 besser als 3:1 ⇨ 2 ⇨ 3.

Intervallskalen ermöglichen die Ordnung auf einer Dimension, wobei die Abstände zwischen den Skalenpunkten gleich sind. So sind 30K wärmer als 20K und wärmer als 10K, wobei die Abstände zwischen allen Temperaturen gleich sind.

Verhältnisskalen ermöglichen die Ordnung auf einer Dimension, wobei die Abstände zwischen den Skalenpunkten gleich sind, zusätzlich gibt es einen festen, nicht willkürlichen Nullpunkt. Eine VP die 20 Jahre alt ist, ist 10 Jahre älter als eine 10-jährige

17 W. D. Fröhlich. Wörterbuch Psychologie. 26. überarb. u. erw. Aufl. 2008, S. 455.

18 D. Wendt. „Statistische Entscheidungstheorie und Bayes-Statistik". In: Hypothesenprüfung. Hrsg. von J. Bredenkamp und H. Feger. 1983, S. 471, 529, S. 471.

19 H.-M. Süß. Einführung in die Forschungsmethoden der Psychologie. 2007, S. 64 f.

VP. Sie ist außerdem doppelt so alt, da die Geburt den Nullpunkt des Lebensalters markiert und damit den Vergleich „doppelt so alt wie“ ermöglicht. Aufgabe der Wissenschaft sei es nun, geeignete Kriterien aufzustellen, die beobachtete Phänomene in eine geeignete, möglichst hochwertige, Skala umwandeln[20]. Dies sei notwendig, um nach wissenschaftlichen Kriterien im Rahmen der Diagnostik, „Differenzen zwischen Merkmalsträgern unter standardisierten Bedingungen zum Zwecke einer diagnostischen Anwendung“ zu erheben. Aus dieser Erhebung könne man dann „bestimmte Schlussfolgerungen, Prognosen oder kontrollierte Maßnahmen ableiten“[21].
Hieraus schließe ich, dass für die Messbarkeit der Sicherheit hochwertige Messverfahren unter standardisierten Bedingungen notwendig sind. Sicherheit in einer Nominalskala zu erfassen ist sinnlos, da dies nur eine simple Zuweisung ist. Es ist zwingend notwendig, dass die Messung die Vergleichbarkeit von Systemen (sicherer als/unsicherer als) ermöglicht, da diese Relation notwendig ist, um Veränderungen (Interventionen) messen zu können. Es kommen also nur noch Ordinal-, Intervall- oder Verhältnisskalen in Frage. Welche Kriterien ein Messverfahren als hochwertig (oder gut oder geeignet) kennzeichnen, werde ich im folgenden diskutieren.
In der Praxis kommen häufig naive Messungen vor, die den wissenschaftlichen Kriterien nicht genügen.
So finden sich zahlreiche Behauptungen[22] zur Sicherheit von Betriebssystemen oder Anwendungsprogrammen, die naiver Natur sind oder den von mir noch aufzustellenden Kriterien nicht genügen. Weiterhin möchte ich überprüfen, ob es möglich ist, Sicherheitsmessungen mit hochwertigen Skalenniveaus durchzuführen, das heißt ob es möglich ist, eine Verhältnisskala zu generieren, die Aussagen der Art „System 1 ist sicherer als System 2 und sicherer als System 3, wobei System 1 doppelt so sicher wie System 3 und 30 % sicherer als System 2 ist“ ermöglichen. So schrieb Heinz von Foerster[23] zum Messen, Rechnen und Ordnen:

> Wenn ich den Begriff des „Rechnens“ verwende, dann beschränke ich ihn nicht auf spezifische Operationen wie z.B. Addition, Multiplikation usw. Ich möchte „Rechnen“ im allgemeinen Sinn als einen Mechanismus oder „Algorithmus“ des Ordnens bzw. der Erzeugung von Ordnung verstehen. Die ideale „oder vielleicht sollte man sagen: die allgemeinste“ Darstellung eines solchen Mechanismus ist natürlich die Turingmaschine, und anhand dieser Maschine möchte ich einige meiner Behauptungen verdeutlichen. Es gibt zwei Ebenen, auf denen wir von „Ordnen“ sprechen können. Einmal wollen wir eine gegebene Anordnung von Gegenständen beschreiben, zum anderen gewisse Dinge entsprechend bestimmten Beschreibungen neu anordnen. Diese beiden Operationen sind in der Tat die Grundlage für all das, was wir „Rechnen“ nennen.

20 Wendt, s. Anm. 2, S. 471.

21 M. Pospeschill und F. M. Spinath. Psychologische Diagnostik. 2009, S. 14.

22 z. B. im Usenet unter Message-ID: <pan.2003.02.25.17.48.59.334523@web.de> oder 3CC5596F.3FFB1294@rz.tu-ilmenau.de oder im WWW unter http://www.heise.de/security/meldung/Hacker-Wettbewerb-Welches-Betriebssystem-ist-das-sicherste-193158.html v. 2011-02-28

23 H. von Foerster. „Die Verantwortung des Experten“. In: Wissen und Gewissen. Versuch einer Brücke. Hrsg. von S. J. Schmidt. 1993, S. 337–346, S. 340.

Ich will also (mit von Foersters Worten) beschreiben, wie man eine Maschine erzeugt, die eine wissenschaftlich fundierte Anordnung für die Sicherheit von IT-Systemen errechnet.

2.2 Der Begriff der Sicherheit

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[24].
Das heißt bezugnehmend auf von Foerster[25], dass die Prämissen eine Maschine erzeugen, die die Sicherheit einer Sache berechenbar macht. Ich stelle daher fest, dass der Begriff Sicherheit normativer Natur ist:

Satz 1 (Sicherheit ist normativ.)

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 (sicher unsicher)[26].

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.

24 vgl. H. Poser. Wissenschaftstheorie. 2001, S. 27 .

25 Von Foerster, „Die Verantwortung des Experten“, s. Anm. 7, S. 340.

26 Das Kreuz ist ein mathematisches Formelzeichen aus G. Spencer-Brown. Laws of Form. Gesetze der Form. 2. Aufl.1999. Ich erläutere seinen Gebrauch näher in Satz 8, Kap. 2.4.

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[27] wie folgt definiert werden:

Vertraulichkeit: Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

27 „Leitfaden IT-Sicherheit IT-Grundschutz kompakt". De. In: (2006). Hrsg. von Bundesamt für Sicherheit in der Informationstechnik. url: http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf (besucht am 16.10.2006), S. 8.

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

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.

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.

Autorisierung: Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

Datensicherheit: Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein anderer Begriff dafür ist „IT-Sicherheit".

Sicherheitsüberprüfungen in der Informatik wenden daher meist die oben genannten VIVA-Kriterien an und überprüfen ein System hinsichtlich deren Einhaltung. Dabei wird in der Regel der Anwender aus der Betrachtung ausgeschlossen. Ich möchte dies am Beispiel des E-Mailsystems erläutern: Alice und Bob möchten vertrauliche Daten per E-Mail austauschen. Wenn sie diese Daten per E-Mail verschicken wollen, müssen sie eine VIVA-Analyse (Diagnose) des E-Mail-Systems durchführen:

Vertraulichkeit E-Mails werden als einfache Textdatei zwischen den Mailservern weitergeleitet. Jeder der Zugriff auf die Mailqueue hat, kann die E-Mails auf einem Server lesen. Ebenso kann der Netzwerkverkehr an zentraler Stelle abgefangen und ausgewertet werden. Jeder der schreibenden Zugriff auf die Mailqueue eines Mailservers hat, kann dort eine Mail verändern. Eine E-Mail ist also nicht integer.

Verfügbarkeit: E-Mails können im Netz abgefangen werden und erreichen den Empfänger daher nicht. Die Verfügbarkeit von E-Mails ist nur eingeschränkt möglich.

Authentizität: Zusammen mit der Integrität kann auch die Authentizität manipuliert werden, das heißt ein Angreifer kann nicht nur den Inhalt der Mail, sondern auch Absender und Zeitstempel ändern. Die Authentizität einer E-Mail ist daher nicht gewährleistet.

Alice und Bob stellen also fest, dass das E-Mailsystem ihren Sicherheitsanforderungen nicht genügt. Sie befassen sich daher mit einem Verschlüsselungssystem für E-Mails und führen nun die Diagnose anhand der VIVA-Kriterien erneut für eine mit GnuPG verschlüsselte Mail durch:

Vertraulichkeit: Eine verschlüsselte E-Mail kann zwar weiterhin abgefangen, aber nicht mehr gelesen werden, solange das Kryptosystem sicher ist.

Integrität: Eine verschlüsselte und signierte E-Mail kann nicht manipuliert werden, solange das Kryptosystem sicher ist.

Verfügbarkeit: Auch verschlüsselte E-Mails können abgefangen und gelöscht werden, die Verfügbarkeit von verschlüsselten E-Mails ist nur eingeschränkt möglich.

Authentizität: Zusammen mit der Integrität schützt die Verschlüsselung und Signatur auch die Authentizität, da der Inhalt der E-Mail nicht verändert werden kann, solange das Kryptosystem sicher ist.

Anhand dieser Diagnose können Alice und Bob feststellen, dass ein verschlüsseltes E-Mailsystem ihren Anforderungen genügt und daher als „sicher“ zu bezeichnen ist. Sie ignorieren hierbei aber die Sicherheit des Kryptosystems. Außerdem ignorieren sie ihre eigenen Entscheidungen bzw. die Entscheidungen der Anwender. So muss jeder Anwender über ein starkes Passwort verfügen und dies geheim halten. Derartige Anforderungen sind sozialer Natur. In der Praxis zeigt sich, dass die Annahme, Benutzer würden ihr Passwort sicher auswählen und geheim halten, nicht zutrifft.
Eine Diagnose anhand der VIVA-Kriterien eignet sich daher nur, um die technische Dimension der Sicherheit zu untersuchen. Die Komplexität der Analyse wird reduziert, indem die soziale Dimension entweder ignoriert wird oder das menschliche Verhalten als wohldefiniert (trivial) gesetzt wird[28]. Somit ist eine Diagnose zwar vergleichsweise einfach durchzuführen und auch in Programmen wie Virenscannern oder Intrusion Detection Systemen[29] implementierbar, dafür ist sie aber schwer generalisierbar, insbesondere in der sozialen Dimension. Die diagnostischen und vor allem prognostischen Fähigkeiten von Computerprogrammen habe ich anhand Jean Piagets genetischer Epistemologie bei Schumacher[30] diskutiert.

28 vgl. N. Luhmann. Vertrauen. 4. Aufl. 2000.

29 vgl. S. Schumacher. Einbruchserkennung in Netzwerke mit Intrusion Detection Systemen und Honeypots. 2005. url:http://www.kaishakunin.com/publ/einbruchserkennung.pdf (besucht am 21. 05. 2008).

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

2.3 Die soziale Dimension der Sicherheit am Beispiel des Social-Engineerings

Eine Besonderheit in der IT-Sicherheitsdebatte sind sogenannte Social-Engineering-Attacken. Hierbei steht Social-Engineering aber nicht für das von Popper[31] vorgestellte Konzept, eine als Ideal vorgestellte Gesellschaftsform mit behavioristischen Methoden zu „engineeren", sondern für Angriffsmethoden[32] auf Systeme, die den Menschen und sein Verhalten zum Ziel haben. Sie spielen also komplett oder, zumindest in Teilen, in der sozialen Ebene. Ich verwende den Begriff Social-Engineering daher in dieser Arbeit als Bezeichnung für Angriffe auf Menschen, in denen diesen mittels verschiedener psychologischer „Tricks" Informationen entlockt oder sie zu bestimmten Handlungen gebracht werden sollen.
Ein Angreifer verwendet dazu im Social-Engineering verschiedene Strategien und Taktiken, um aus Benutzern der Systeme Informationen wie Passwörter oder IP-Adressen herauszuholen. Mithilfe dieser Informationen kann er erfolgreiche Angriffe gegen Zielsysteme fahren.
Social-Engineering ist äußerst erfolgreich, wenn größere Organisationen wie Unternehmen, Behörden oder Universitäten angegriffen werden sollen. Oftmals gelingt es einem Angreifer mit der Aggregation öffentlich zugänglicher Informationen und entsprechender Kaltschnäuzigkeit wichtige Informationen und Zugriff auf geschützte Systeme zu erlangen. Eine weitverbreitete und bekannte Form des Social-Engineerings ist das sogenannte Phishing, bei dem mit gefälschten Emails oder manipulierten Webseiten Benutzer dazu verleitet werden sollen, Logindaten zu ihren Bank- oder E-Mailkonten anzugeben. Derartige Angriffe sind sehr leicht durchzuführen, da der Angreifer dazu lediglich etwas Webspace benötigt und dort die entsprechende Webseite nachahmt. Das „richtige" Social-Engineering, Human Based Social-Engineering genannt, setzt zum Großteil oder komplett auf soziale Beziehungen als Angriffsvektor.
Zuerst benötigt der Angreifer möglichst viele Informationen über die anzugreifende Organisation. Diese kann er aus freien Informationen, wie beispielsweise der Webseite oder Werbebroschüren, zusammensammeln und sich so ein Bild machen. Er kann auch den Müll durchwühlen und so an relevante Daten kommen. Außerdem können gewieftere Angreifer über E-Mail oder Telefon Kontakte zu Mitarbeitern herstellen und sich als ein Kunde oder Vorgesetzter ausgeben, der dringend Informationen benötigt. Mit diesen kann er dann andere Opfer beeindrucken oder einwickeln. Vorsicht ist daher mit der Freigabe von Informationen geboten, auch solchen, die auf den ersten Blick unverfänglich erscheinen. So mag es für die Mitarbeiter nützlich sein, dass alle Mitarbeiter des Rechenzentrums inklusive Telefonnummer, Emailadresse, Aufgabengebiet und Foto auf einer Webseite aufgeführt werden. Wird diese Seite jedoch weltweit freigegeben, kann sich ein Angreifer sehr nützliche Informationen über die Struktur des Rechenzentrums beschaffen. So kann er anderen Mitarbeitern am Telefon beispielsweise intime Kenntnisse des Betriebs vorgaukeln oder schneller

31 K. Popper. The Open Society and Its Enemies. Bd. 1: The Spell of Plato. 2 Bde. 1945.

32 Dieses Kapitel ist eine überarbeitete und angepasste Version von Teilen früherer Veröffentlichungen von mir, welche im Text aufgeführt sind. [SS]

Kontakte knüpfen. Weiß der Angreifer beispielsweise, dass ein Mitarbeiter Pferdenarr ist, kann er Termindruck vortäuschen, weil sein eigenes Pferd dringendst zum Tierarzt muss. Das Opfer der Attacke wird als Pferdefreund Sympathie für den Angreifer empfinden und versuchen ihm zu helfen.

Dieses Sympathie-Aufbauen lässt sich auf verschiedenen Wegen durchführen, beispielsweise mit der Verbrüderung von Opfern, indem man einen gemeinsamen Gegner vorgibt: „Die im Rechenzentrum haben wieder mal den Server abstürzen lassen" oder „Das dumme Word hat mal wieder die Datei zerstört" führen in der Regel zur Solidarität des Opfers und damit möglicherweise zur Herausgabe der Daten.

Andere Maschen sind Vorspiegelung von Autorität, was insbesondere in strengen Hierarchien wie Polizei, Armee oder Feuerwehr sehr gut funktioniert. Selbst jemand der nur Grundwehrdienst geleistet hat, kann mit etwas Geschick und Witz als Offizier auftreten und eine Dienststelle erfolgreich infiltrieren, wie es der arbeitslose Schuhmacher Voigt als „Hauptmann von Köpenick" vorgemacht hat. Durch die zusammengekaufte Uniform eines Hauptmanns gelang[33] es ihm zuerst einen Trupp von zehn Soldaten unter sein Kommando zu stellen und mit diesen das Köpenicker Rathaus zu besetzen. Anschließend „verhaftete" er unter anderem den Bürgermeister und „beschlagnahmte" die Stadtkasse unter Hinweis auf Abrechnungsunregelmäßigkeiten. Dabei nutzte er die Hauptmannsuniform als Symbol seiner Autorität.

Aber auch in normalen Unternehmen gibt es Hierarchien, die sich ausnutzen lassen, so kann sich der Angreifer als wichtiger Kunde oder hoher Verantwortlicher einer anderen Filiale ausgeben. Unter Aufbau einer passenden Drohkulisse „Wenn wir ihretwegen den Kunden verlieren, dann . . . !", „Es kann ja wohl nicht sein, das Sie Ihren Laden nicht beisammen haben und mir die Akten nicht geben wollen!" oder „Wenn das Dr. Müller-Lüdenscheid bei unserem nächsten Golfturnier erfährt, wird er bestimmt sehr sauer sein!" kann man hier Mitarbeiter zur Herausgabe von Daten bewegen.

Für die weitere Diskussion ist hierbei wichtig, dass über soziale Angriffe, technische Angriffe vorbereitet werden können bzw. es auch möglich ist, durch reines Social-Engineering à la Hauptmann von Köpenick erfolgreich Daten oder Gegenstände erbeuten kann. Es ist außerdem wichtig, das technische Maßnahmen Social-Engineering zwar erschweren, nicht aber komplett verhindern können. Dies werde ich im folgenden noch genauer diskutieren. Wie Social-Engineering-Angriffe im Detail funktionieren, habe ich ausführlich in „Psychologische Grundlagen des Social-Engineering"[34]

33 http://de.wikipedia.org/wiki/Hauptmann_von_Köpenick v. 2011-03-03

34 S. Schumacher. „Psychologische Grundlagen des Social-Engineering". In: Proceedings des GUUG Frühjahrsfachgespräches 2009. (Hochschule Karlsruhe). Hrsg. von German Unix User Group. Berlin: Lehmanns Media, 2009, S. 77 98; S. Schumacher. „Admins Albtraum. Die psychologischen Grundlagen des Social Engineering, Teil I". In: Informationsdienst IT-Grundschutz 7 (2009), S. 11–13. url: http://grundschutz.info/fileadmin/kundenbereich/Dokumente/ Grundschutz_7-2009_11_13.pdf (besucht am 22. 07. 2009); S. Schumacher. „Admins Albtraum. Die psychologischen Grundlagen des Social Engineering, Teil II". In: Informationsdienst IT-Grundschutz 8 (2009), S. 8 - 9. url: http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_8-2009_8_9.pdf (besucht am 24. 08. 2009); S. Schumacher. „Admins Albtraum. Die psychologischen Grundlagen des Social Engineering, Teil III". In: Informationsdienst IT-Grundschutz 10/11 (2009), S. 21–22; S. Schumacher. „Psychologische Grundlagen des Social-Engineering". In: Die Datenschleuder. Das wissenschaftliche Fachblatt für den Datenreisenden #94 (2010). Hrsg. von Chaos Computer Club, S. 52–59. url: http://ds.ccc.de/pdfs/ds094.pdf (besucht am 10. 10. 2010).

diskutiert und dort insbesondere auch die sozialpsychologischen Grundlagen vorgestellt. Weiterführende Literatur zu Social-Engineering-Attacken finden sich vor allem bei Witnick und Simon35 und R. B. Cialdini. „Die Psychologie des Überzeugens“ (2007).
In Satz 2 unterscheide ich zum Zwecke der theoretischen Diskussion technische, soziale und technisch soziale Angriffe. In der Praxis lässt sich jeder Angriff als technisch-sozialer Angriff beschreiben, da in irgendeiner Form immer Entscheidungen eines Menschen eine Rolle spielen, es also eine soziale Ebene gibt. Im Rahmen der theoretischen Diskussion möchte ich zunächst dennoch diese Begriffe einführen, um mit ihnen weitere Sätze herzuleiten. bzw. zu verdeutlichen.

Satz 2 (technische und soziale Angriffe)

α. Ein Angriff auf rein technischer Ebene heiße technischer Angriff.

β. Ein Angriff auf rein sozialer Ebene heiße sozialer Angriff.

γ. Technische und soziale Angriffe können kombiniert werden, der kombinierte Angriff heiße technisch-sozialer Angriff.

2.4 Der Begriff der Berechenbarkeit

Dem Begriff „Berechenbarkeit“ können verschiedene Konzepte zu Grunde liegen. So befassen sich die theoretische Informatik und mathematische Logik im Fachgebiet der Berechenbarkeitstheorie damit, welche Probleme mithilfe eines mathematischen Modells algorithmisierbar sind. Dies ist notwendig, da Computer nur Algorithmen berechnen können. Ist eine Fragestellung nicht algorithmisierbar, kann sie nicht von einem Computer berechnet werden. Daher ist es wichtig zu klären, was Algorithmisierbarkeit bedeutet und welche Probleme algorithmisiert werden können. Daraus lässt sich schlussfolgern, in welchen Dimensionen Computer zur Berechnung von Sicherheit eingesetzt werden können, also ob sie beispielsweise auch in der Lage sind, menschliches Verhalten adäquat zu berechnen und damit vorherzusagen.
Der englische Mathematiker Alan Turing formalisierte während des Zweiten Weltkrieges[36] mathematische Berechnungsvorschriften mit dem Modell der Turingmaschine, welche formal als 7-Tupel definiert ist[37]:

35 K. Mitnick und W. Simon. Die Kunst der Täuschung. 2006, S. 400; K. Mitnick und W. Simon. Die Kunst des Einbruchs. 2006, S. 334.

36 Turing arbeitete in Bletchley Park daran die deutsche Verschlüsselungsmaschine Enigma zu brechen. Die Formalisierung der Berechenbarkeitstheorie wurde also direkt von einer Sicherheitsanalyse getrieben.

37 vgl. R. Stiebe. Theoretische Informatik für Ingenieur-Informatiker. 2003.

1. $M = (Q, \sum, \Gamma, \delta, q_0, \square, q_f)$:= formales 7-Tupel
2. Q := endliche Zustandsmenge
3. $\sum$:= Eingabealphabet
4. Γ := endliches Bandalphabet mit $\sum \subset \Gamma$ $\square$
5. . $\delta: (Q \setminus \{ q_f \}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, 0, R\}$:= partielle Überführungsfunktion
6. $q_0 \in Q$:= Anfangszustand
7. $\square \in \Gamma \setminus \sum$:= leeres Feld
8. $q_f \in Q$:= akzeptierende Zustand

Die Turingmaschine ist eines der zentralen Konzepte der (theoretischen) Informatik und wird im allgemeinen dazu verwendet, den Begriff Algorithmus zu definieren. Ein Algorithmus muss daher folgenden Kriterien genügen:

Finitheit: Der Algorithmus muss in einer endlichen Vorschrift eindeutig beschreibbar sein.

Ausführbarkeit: Jeder Schritt des Algorithmus muss ausführbar sein.

Platzkomplexität: Der Algorithmus darf nur endlich viel Speicherplatz erfordern.

Zeitkomplexität: Der Algorithmus darf nur endlich viele Schritte erfordern.

Determiniertheit: Der Algorithmus muss bei den gleichen Eingaben die selben Ausgaben liefern.

Determinismus: Die nächste anzuwendende Berechnungsvorschrift ist jederzeit eindeutig definiert.

Genügt eine Berechnungsvorschrift diesen Kriterien nicht, ist sie kein Algorithmus und kann daher auch nicht mit einem Computer (sinnvoll) ausgeführt werden[38].
Besondere Bedeutung bekommen hier die Kriterien Determiniertheit und Determinismus. Determiniertheit bedeutet, dass der Algorithmus angewendet auf den selben Input immer den selben Output ergibt. Egal wer, wann, wo, wie und womit den Algorithmus Quadratwurzel von X ($\sqrt{X}$) anwendet, wenn er als Input eine 9 wählt,

38 vgl. G. Saake und K.-U. Sattler. Algorithmen und Datenstrukturen. Eine Einführung mit Java. 2002, Kap. 2 "Algorithmische Grundkonzepte".

kommt immer 3 als Ergebnis heraus. Ein komplexerer Algorithmus wie beispielsweise die Fakultät einer Zahl ist wie folgt definiert: n! =1 * 2 * 3 : : : * n =k=1nk. Das heißt, dass die Fakultät das Produkt einer Zahl und aller ihrer Vorgänger ist, 4! = 2 * 3 * 4 = 24. Der Algorithmus n! liefert bei der selben Eingabe die selbe Ausgabe und der nächste anzuwendende Schritt ist jederzeitig eindeutig definiert: multipliziere das Zwischen-Ergebnis mit dem Nachfolger der aktuellen Zahl, wenn diese kleiner gleich der Eingabe ist, sonst brich ab. Die Berechnungsvorschriften Quadratwurzel und Fakultät sind somit deterministische und determinierende Algorithmen.
Die Berechnungsvorschrift f (x) = (2 * 3 * x)+PRNG ist nicht-deterministisch, da die Funktion PRNG einen Pseudozufallsgenerator (pseudo random number generator) darstellt, also bei jedem Aufruf eine pseudozufällig gewählte Zahl ausgibt. Alternativ könnte man auch das Ergebnis eines Würfelwurfs einsetzen. Daher wird bei jedem Aufruf des Algorithmus ein anderes Ergebnis zurückgegeben, welches nicht vorhergesagt werden kann. Derartige Algorithmen werden als nicht-deterministisch (oder auch probabilistisch) bezeichnet. Sie spielen beispielsweise in der Kryptographie eine Rolle, sind aber durch eine Turingmaschine nicht berechenbar.
Das Algorithmen- bzw. Berechenbarkeitsparadigma ist notwendig, um die Funktion von Computern und Computerprogrammen zu verstehen. Computerpgrogramme und Computerhardware lassen sich als Turingmaschine modellieren und sind daher nur in der Lage Algorithmen auszuführen. Sie können problemlos mathematische Algorithmen lösen, nicht aber echte Zufallszahlen generieren, einen Text hermeneutisch analysieren oder gar menschliches Verhalten vorhersagen. Daher ist es nicht möglich, menschliches Verhalten von einem Computerprogramm überwachen zu lassen, es sei denn, das Verhalten ist algorithmisiert, also hochgradig standardisiert. Daher kann ein Computerprogramm maximal in der technischen Dimension eingesetzt werden, um Sicherheit zu messen, beispielsweise in Form eines Virenscanners oder Intrusion Detection Systems[39].
Heinz von Foerster, einer der Mitbegründer der Kybernetik und Vertreter des radikalen Konstruktivismus, befasste sich in seinem Gesamtwerk unter anderem mit der Funktionsweise des Gedächtnisses, kybernetischen Steuerungsmechanismen in der Funktechnik und später damit, wie diese technische Kybernetik auf soziale und psychische Systeme übertragen werden kann.
Ein zentraler Punkt seiner Werke ist die Entscheidbarkeit oder Berechenbarkeit von Entscheidungen. Er greift darauf in vielen seiner Arbeiten[40] zurück, verwendet dabei jedoch unterschiedliche Terminologien, da er meist in einzelnen Artikeln oder Buchkapiteln publiziert und kein zentrales Opus Magnum vorgelegt hat. Daher greife ich

39 vgl. Schumacher, „Auf dem Weg zum Intrusion Detection System der nächsten Generation“, s. Anm. 14 Schumacher, Einbruchserkennung in Netzwerke mit Intrusion Detection Systemen und Honeypots, s. Anm. 13.

40 vgl. H. von Foerster. „Ethik und Kybernetik zweiter Ordnung“. In: Kurzzeittherapie und Wirklichkeit. Hrsg. von P. Watzlawick und G. Nardone. 2008, S. 71–89; H. von Foerster und B. Pörksen. Wahrheit ist die Erfindung eines Lügners. Gespräche für Skeptiker. 7. Aufl. 2006; H. von Foerster. „Betrifft: Erkenntnistheorien“. In: Wissen und Gewissen. Versuch einer Brücke. Hrsg. von S. J. Schmidt. 1993, S. 364–370; H. von Foerster. „Was ist Gedächtnis, daß es Rückschau und Vorschau ermöglicht?“ In: Wissen und Gewissen. Versuch einer Brücke. Hrsg. von S. J. Schmidt. 1993, S. 299–336.

auf ein Zitat von Baecker[41] zurück, um Foersters Ansatz zu beschreiben:
In der kybernetischen Forschung unterscheidet man wohl-definierte und schlecht-definierte Systeme. Wohldefinierte Systeme sind dadurch gekennzeichnet, dass alle möglichen Übergänge zwischen den verschiedenen Zuständen, die sie einnehmen können, bekannt sind; dass die Wahrscheinlichkeit dieser Übergänge bekannt ist; und dass sich weder die Übergänge noch die Zustände in Abhängigkeit von der Zeit ändern. Heinz von Foerster würde von einer trivialen Maschine sprechen, die synthetisch determiniert, analytisch determinierbar und historisch unabhängig ist. Schlecht-definierte Systeme hingegen sind dadurch definiert (!), dass die möglichen Übergänge zwischen verschiedenen Zuständen unbekannt sind; dass die Wahrscheinlichkeit dieser Übergänge unbekannt ist; und dass sich sowohl die Übergänge als auch die Zustände und nicht zuletzt die Wahrscheinlichkeit der Übergänge und Zustände in Abhängigkeit von der Zeit ändern. Heinz von Foerster würde von nichttrivialen Maschinen sprechen, die synthetisch determiniert, aber analytisch undeterminierbar und historisch abhängig sind.
Die Turingmaschine ist somit in der Terminologie von Foersters eine wohl-definierte Maschine, die nur wohldefinierte Programme (in der theoretischen Informatik "Algorithmus" genannt) erfolgreich berechnen kann, sie ist also ebenso wie ein Algorithmus trivial. Ich definiere daher bezugnehmend auf[42] triviale Maschinen und Probleme:

Eine triviale Maschine hat folgende Eigenschaften:

α. Alle Zustandsübergänge sind bekann.t

β. Die Eintrittswahrscheinlichkeiten aller Zustandsübergänge sind bekannt.

γ. Zustandsübergänge und deren Eintrittswahrscheinlichkeiten ändern sich mit der Zeit nicht,die Maschine ist daher:

δ. synthetisch determiniert,

ε. analytisch determinierbar,

ζ. historisch unabhängig.

Satz 4 (Nicht-Triviale Maschine)
Eine nicht-triviale Maschine hat folgende Eigenschaften:

α. Nicht alle Zustandsübergänge sind bekannt.

β. Die Eintrittswahrscheinlichkeiten der Zustandsübergänge sind unbekannt.

41 D. Baecker, Hrsg. Organisation als System. 3. Aufl. 2005, S. 15 f.

42 Ebd., S. 15 f.

γ. Zustände, Zustandsübergänge sowie deren Eintrittswahrscheinlichkeiten ändern sich mit der Zeit nicht, die Maschine ist daher:

δ. synthetisch determiniert,

ε. analytisch undeterminierbar,

ζ. historisch abhängig.

Satz 5 (Triviales Problem)
Ein Problem ist trivial, wenn es von einer trivialen Maschine berechnet werden kann.

Satz 6 (Nicht-Triviales Problem)
Ein Problem ist nicht-trivial, wenn es nicht von einer trivialen Maschine berechnet werden kann.

Da die Zustandsübergänge im Geiste eines Menschen ebenso unberechenbar sind wie deren Eintrittswahrscheinlichkeit oder ihre Abhängigkeit von der Zeit, sind Menschen in ihren Entscheidungen nichttrivial. Wären Menschen triviale-Maschinen ließe sich ihr Verhalten turing-berechnen und beispielsweise über algorithmisierbare Reiz-Reaktions-Ketten beschreiben. Das hieße, dass alle Studenten, die eine Vorlesung regelmäßig besucht haben, in der abschließenden Klausur die selben Ergebnisse erzielen müssten, schließlich haben alle „Maschinen" den selben Input bekommen und mit der Klausur auch die selbe Berechnungsvorschrift.
Dass Menschen nicht-trivial sind, hat nicht nur Heinz von Foerster geschlussfolgert, sondern neben ihm auch N. Chomsky[43], J. Piaget[44] und P. Watzlawick. „Selbsterfüllende Prophezeiungen". In: Die erfundene Wirklichkeit. Hrsg. Von P. Watzlawick. 4. Aufl. 2008, S. 91–110. Diese Werke legten neben anderen auch den Grundstein für den pädagogischen Kompetenzbegriff.

Satz 7 (Der Mensch als Maschine)
Der Mensch ist eine nicht-triviale Maschine. Er kann sowohl triviale als auch nicht-triviale Entscheidungen treffen.

In der Kybernetik wird ebenso wie in der soziologischen Systemtheorie auf George Spencer-Browns „Gesetze der Form" zurückgegriffen[45].

43 N. Chomsky. „Explanatory models in linguistics". In: Logic, methodology, and philosophy of science. Hrsg. von E. Nagel, P. Suppes und A. Tarski. 1962, S. 528 - 550.

44 J. Piaget. Einführung in die genetische Erkenntnistheorie. Jan. 1996.

45 H. von Foerster. „Über das Konstruieren von Wirklichkeiten". In: Wissen und Gewissen. Versuch einer Brücke. Hrsg. von S. J. Schmidt. 1993, S. 25–49; H. Maturana und F. Varela. Der Baum der Erkenntnis. Die biologischen Wurzeln des menschlichen Erkennens. 2. Aufl. 2009; H. Maturana. Biologie der Realität. 1998; H. Maturana und F. Varela. Autopoiesis and Cognition. The Realization of the Living. 1980; D. Baecker. „Wenn es im System rauscht". In: Organisation als System. Hrsg. von D. Baecker. 3. Aufl. 2005, S. 38–50; N. Luhmann. Soziologie des Risikos. unveränderter

Darin erzeugt[46] auf 120 Seiten einen formalen Kalkül, dessen Grundlage „Triff eine Unterscheidung“ lautet. Die Mächtigkeit[47] des formalen Kalküls entspricht nach Spencer-Brown der Mächtigkeit der Principia Mathematica von Bertrand Russell und Alfred North Whitehead.
Für das Thema dieser Arbeit, genügt es, lediglich die Unterscheidung und deren Formelzeichen einzuführen. Mit Brown[48] definiere ich:

Satz 8 (Triff eine Unterscheidung)

α. Der Zustand der Außenseite der Markierung ist nicht der Zustand der Innenseite der Markierung.

β. Die Markierung der Unterscheidung sei ein genannt Cross oder Kreuz.

γ $\overline{a|}: \neg a; \overline{\text{Innen}|}\text{Außen}$

Nach dem ich also nun festgestellt habe, was triviale und nicht-triviale Entscheidungen sowie Maschinen sind, möchte ich diese Begriffe im Rahmen einer Sicherheitsanalyse anwenden, um zu untersuchen wie Sicherheit gemessen werden kann. Die Buchhalterin Alice verfügt über ein eigenes Login/Passwort im Online-Bankingsystem ihres Unternehmens.
Darüber kann Sie Zahlungen veranlassen, beispielsweise um die Forderungen von Lieferanten zu begleichen. Das Passwort hat sie selbst gewählt. Im Falle einer unberechtigten Überweisung kann die Bank anhand der Login-Daten nachverfolgen, wer die Überweisung wann und von welcher IP-Adresse aus getätigt hat. Diese Daten unterliegen vor Gericht zwar der freien Beweiswürdigung, führten aber schon des öfteren zu Verurteilungen. Wenn Alice nun eine Überweisung durchführen will, muss sie folgende Schritte durchführen:

1. Am eigenen Arbeitsplatz anmelden und einen Webbrowser starten.
2. Im Webbrowser die korrekte URL für das Bankingsystem angeben.
3. Das kryptographische Zertifikat des Systems muss überprüft werden, um sicherzustellen, das Alice auch wirklich mit der Bankingseite und nicht mit einer gefälschten Seite kommuniziert.
4. Allice logt sich mit ihrem Nutzernamen und Passwort bei der Bank ein.
5. Sie tätigt eine Überweisung und gibt die notwendige TAN von ihrer TAN-Liste ein.

Im Rahmen einer technischen Sicherheitsanalyse (die ich hier nur stark verkürzt wie-

Nachdruck der Ausgabe von 1991. 2003.

46 Spencer-Brown, s. Anm. 10.

47 Der formale Beweis bleibt dem Leser zur Übung überlassen. [SS]

48 Spencer-Brown, s. Anm. 10, S. 3.

dergebe, denn die technische Sicherheit steht nicht im Mittelpunkt dieses Aufsatzes), würde ich folgende Punkte untersuchen:

- Ist das von der Bank eingesetzte Verschlüsselungsverfahren stark genug, oder werden schwache oder veraltete Algorithmen eingesetzt?
- Ist das von Alice gewählte Passwort stark genug?

Beide Fragen beziehen sich vordergründig auf technische Fragen. So würde ich die eingesetzten Verschlüsselungsverfahren nicht selber evaluieren, da mir hierzu die Handlungskompetenz fehlt, ich würde stattdessen in der einschlägigen Literatur den „gegenwärtigen Stand der Technik" recherchieren und überprüfen ob das Bankingsystem diesen Anforderungen genügt.
Ebenso kann ich das von Alice gewählte Passwort trivial überprüfen: Hat es eine sinnvolle Mindestlänge? Ist es ein normales Wort, das mit einer Wörterbuchattacke erraten werden kann? Verwendet es Sonderzeichen, Zahlen sowie Groß- und Kleinschreibung? Hat Alice es in den letzten 60 Tagen gewechselt?
Diese Gütekriterien für ein Passwort lassen sich aufstellen, in dem man es im Rahmen eines Penetration-Tests, also einem Einbruchsversuch zu Testzwecken, angreift. Dazu verwendet man die selben Werkzeuge und Methoden, die auch bösartige Angreifer nutzen. So kann man mit ein wenig Kombinatorik eine sinnvolle Mindestlänge für ein Passwort berechnen, dies wird in der Informatik im Rahmen einer sogenannten Aufwandsabschätzung gemacht. Mithilfe der Mindestlänge und der Definition eines Grundalphabets definiert man so das Gütekriterium „Brechbarkeit" eines Passworts. Mithilfe der Definition des Gütekriteriums hat man so einen Bewertungsrahmen für die „Stärke" eines Passworts erschaffen. Damit umgeht man das Problem des naturalistischen Fehlschlusses (normative Bewertung deskriptiver Daten)[49].
Die Anzahl aller verfügbaren Passwörter ergibt sich aus der Anzahl der verfügbaren Buchstaben im Grundalphabet potenziert mit der Passwortlänge. Eine EC-Karten-Pin mit 4 Stellen und 10 Ziffern hat daher 104 == 10.000 mögliche Kombinationen (0000-9999). Wenn ich nun einen sogenannten Cracker nehme, der systematisch Passwörter durchprobiert, kann ich berechnen wie lange er benötigt um eine EC-PIN im schlimmsten Fall zu knacken. Dazu muss ich nur die Anzahl der PIN-Kombinationen kennen und wissen wie lange das Programm braucht um eine Kombination zu testen. Benötigt es beispielsweise eine Sekunde pro PIN, so dauert das Brechen der PIN 10.000 PINS mal 1 Sekunde, also 10.000 Sekunden, das heißt nicht ganz 3 Stunden.
Erhöhe ich nun die kombinatorische Komplexität der PIN oder des Passwortes hinreichend, benötigt auch das Crack-Programm entsprechend länger. Ein Passwort der Länge 10 und einem Grundalphabet von 99 Zeichen ergibt 9910, also 90.438.207.500.880.449.001 mögliche Kombinationen. Angenommen der Cracker kann 5.000 Passwörter pro Sekunde, also 432.000.000 pro Tag, durchraten, benötigt er im schlimmsten Fall 570.000 Jahrtausende um das Passwort zu cracken. Man kann

49 vgl. Poser, s. Anm. 8.

also davon ausgehen, dass ein Passwort sicher ist, wenn es mindestens zehn Zeichen lang ist und aus verschiedenen Zeichenklassen besteht. Durch die empirisch-experimentelle Erstellung dieser Vorschrift (Das Passwort sei mindestens zehn Zeichen lang und zufällig aus einem Grundalphabet von 99 Zeichen erzeugt), habe ich einen Berechnungsrahmen für das Gütekriterium „Brechbarkeit" des Passwortes erstellt. Dieser Berechnungsrahmen trivialisiert das Gütekriterium soweit, dass ich es mithilfe einer trivialen Maschine, also einem Algorithmus und damit einem Computer, berechnen kann. Dies wird in der Praxis auch gemacht, so kann ich als Systemadministrator beispielsweise das Pluggable-Authentication-Module-Framework (PAM) nutzen, um Gütekriterien für Passwörter festzulegen. So kann ich konfigurieren, das alle Benutzer ihre Passwörter innerhalb eines bestimmten Zeitrahmens wechseln und dass das Passwort eine bestimmte Mindestlänge hat sowie verschiedene Zeichenklassen verwendet. Sollte der Benutzer ein Passwort einstellen wollen, dass diesen Gütekriterien nicht genügt, wird es zurückgewiesen. Die trivial-Maschine Computer zwingt also die nichttrivial-Maschine Mensch etwas so zu tun, wie sie es für richtig hält[50].
Nach Weber[51] unterwirft sich hier der Anwender der „legalen Herrschaft kraft Satzung" in Form der Bürokratie. Wobei anzumerken ist, dass formal der Systemadministrator, der die Passwort-Regeln festlegt formal die Herrschaft übernimmt[52].
Die Bürokratisierung ist aber insbesondere nach Baecker[53] sowie nach Luhmann[54] spätestens bei der Diskussion Sicherheit auf organisationaler Ebene weiter zu untersuchen, da sie zwar Entscheidungen vorwegnimmt, damit eine Organisation aber wiederum angreifbarer macht. Sie sorgt laut Baecker[55] dafür, die traditionelle und charismatische, und damit willkürliche, Herrschaft zu verschriftlichen und Verhalten bzw. Entscheidungen vorhersagbar zu machen. Da die Organisationsmitglieder von ihren Interaktionspartner auch außerhalb der Organisation ein ähnliches Verhalten erwarten, ermöglichen Sie einem Angreifer so, sich mit etwas Kenntnis der Organisation anzupassen und sich als Organisationsmitglied auszugeben. Dadurch kann ein Angreifer an Informationen für weitere Social-Engineering-Attacken oder technische Angriffe gelangen.
Ein weiteres Gütekriterium für ein Passwort ist dessen Geheimhaltung. Niemand

50 Für richtig halten ist hier nur eine Metapher. Natürlich denkt der Computer ebenso wenig wie er etwas für richtig bewertet.

51 M. Weber. „Wirtschaft und Gesellschaft". In: Grundriss der Sozialökonomik. 3te Auflage. Bd. 1. 1947. url: http: //gallica2.bnf.fr/ark:/12148/bpt6k94382s.download (besucht am 13. 04. 2008); M. Weber. „Wirtschaft und Gesellschaft" In: Grundriss der Sozialökonomik. 3te Auflage. Bd. 2. 1947. url: http://gallica2.bnf.fr/ark:/12148/ bpt6k943834.download (besucht am 13. 04. 2008).

52 Auch wenn dies J. Weizenbaum. Die Macht der Computer und die Ohnmacht der Vernunft. 17. Aufl. 2003, Kap. „Die Naturwissenschaft und der zwanghafte Programmierer" und P. Watzlawick, Hrsg. Die erfundene Wirklichkeit. 4. Aufl. 2008, Kap. „Der vielarmige Bandit" anders dargestellt haben und davon ausgehen, dass der Anwender mit dem Computersystem interagiert und dessen charismatische Herrschaft akzeptiert, und ich beiden Autoren aufgrund meiner Erfahrung als Systemadministrator zustimmen möchte, würde diese Diskussion den Rahmen der Arbeit sprengen.

53 D. Baecker. „Die doppelte Schließung der Organisation". In: Organisation als System. Hrsg. von D. Baecker. 3. Aufl.2005, S. 126 - 168, S. 136 .

54 N. Luhmann. Zweckbegriff und Systemrationalität. 11. Aufl. 1999; N. Luhmann. Legitimation durch Verfahren. 12. Aufl. 2008.

55 D. Baecker. „Zum Problem des Wissens in Organisationen". In: Organisation als System. Hrsg. von D. Baecker. 3. Aufl. 2005, S. 68 - 101.

anderes als der berechtigte Benutzer, hier Alice, darf das Passwort kennen. Weder Vorgesetzte, Kollegen oder Familienangehörige und erst recht keine unbekannten Anrufer. Die Einhaltung dieses Gütekriteriums kann weder von einem Computer noch einem Sicherheitsbeauftragten bewiesen werden – sie kann höchstens durch einen Gegenbeweis falsifiziert werden[56]. Dadurch ist die Einhaltung des Gütekriteriums nicht trivial berechenbar, außerdem liegt es in der psychischen/sozialen Dimension. Es kommt einzig und allein darauf an, das Alice das Passwort geheim hält, sie also sicherheitskompetent handelt.
Ich habe mit diesem Beispiel gezeigt, dass sich Sicherheit in die technische und psychische Ebene erstrecken. Da sie sich auch in die psychische Ebene erstreckt und vom nicht-trivialen Verhalten eines Individuums abhängt, ist Sicherheit nicht-trivial. Damit sind die Propositionen 2 und 3 bestätigt.

Satz 9 (Sicherheit ist multi-dimensional)
Sicherheit beschränkt sich nicht auf die technische Dimension, sondern erstreckt sich in die psychische Dimension.

Satz 10 (Sicherheit ist nicht-trivial)
Sicherheit hängt von den Entscheidungen eines Individuums ab, sie ist daher nicht-trivial. Sicherheit kann also auch nicht durch Trivial-Maschinen berechnet werden.

Sicherheit ist also in meinem Modell multi-dimensional. In folgenden werde ich daher die soziale Dimension, also das Verhalten der Menschen, betrachten.

3 Sicherheitskompetenz

3.1 Handlungen, Fähigkeiten, Fertigkeiten und Kenntnisse

In den vorangegangenen Kapiteln habe ich gezeigt, dass IT-Sicherheit nicht-trivial (Sätze 10 und 9) sowie multidimensional (Satz 2) ist und in der psychischen Dimension von den Entscheidungen eines Individuums abhängt. 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

56 vgl. W. Detel. Erkenntnis- und Wissenschaftstheorie. 2008.

Freiheit von unvertretbaren Risiken definiert[57].
Nach Beck[58] bedeutet Risiko

> die Antizipation[59] 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[60].
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[61] 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 wirkliche „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[62] wie folgt definiert werden: „Handlung[63] 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 Operati-

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

58 Beck, s. Anm. 11

59 Hervorhebungen im Original [SS]

60 vgl. dazu insbesondere Schumacher, „Auf dem Weg zum Intrusion Detection System der nächsten Generation", s. Anm. 14

61 W. Hacker. Allgemeine Arbeitspsychologie. 2., vollst. überarb. u. erg. A. 2005, S. 63.

62 Ebd., S. 68 ff

63 Hervorhebungen im Original [SS]

on 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[64]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 sensumotorischem 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 Aufgabe 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)[65]. Diese Entwicklung wurde durch die Automatisierung und PC-Revolution noch dramatisch verschärft, 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, Fer-

64 J. Erpenbeck und W. Sauter. Kompetenzentwicklung im Netz: New Blended Learning mit Web 2.0. 2007, S. 67f.

65 vgl. D. Mertens. „Schlüsselqualifikationen. Thesen zur Schulung für eine moderne Gesellschaft". In: Mitteilungen aus der Arbeitsmarkt- und Berufsforschung 7 (1 1974), S. 36–43. http://doku.iab.de/mittab/1974/1974_1_MittAB_ Mertens.pdf (besucht am 22. 05. 2009).

tigkeiten und Kenntnisse. Am Ende des Kapitels werde ich diese Aussagen durch ein Anwendungs-Beispiel belegen.

3.2 Kompetenz

Den einen Kompetenzbegriff gibt es eben sowenig wie es den einen Wissensbegriff gibt. Die Kompetenzdiskussion hat in Deutschland zu verschiedenen Kompetenzbegriffen und -definitionen geführt.
So definiert Gessler[66]: „Kompetenz befähigt einen Menschen zu selbstverantwortlichem Handeln und bezeichnet den tatsächlich erreichten Lernerfolg. Qualifikation ermöglicht die Verwertung von Kenntnissen, Fertigkeiten und Fähigkeiten".
Kauffeld, Frieling und Grote[67] 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, Kailer und Kottmann[68] 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, indem 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, dass 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[69] habe ich mich eingehender mit dem Kompetenzbegriff von Kanning[70] befasst. Er schreibt:

> „Kompetenzen 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."

66 M. Gessler. „Das Kompetenzmodell". In: Handbuch Personalentwicklung Die Praxis der Personalbildung, Personalförderung und Arbeitsstrukturierung. Hrsg. von R. Bröckermann und M. Müller-Vorbrüggen. 2006, S. 23–42, S. 26.

67 S. Kauffeld, S. Grote und E. Frieling. „Das Kasseler-Kompetenz-Raster (KKR)". In: Handbuch Kompetenzmessung. Hrsg. von J. Erpenbeck und L. von Rosenstiel. 2003, S. 261 - 281, S. 261.

68 E. Staudt, N. Kailer und M. Kottmann. Kompetenzentwicklung und Innovation. 2002, S. 440.

69 S. Schumacher. Soziale Kompetenzen für Informatiker. Otto-von-Guericke-Universität Magdeburg, 2008

70 U. P. Kanning. „Soziale Kompetenzen in der Personalentwicklung". In: Förderung sozialer Kompetenzen in der Personalentwicklung. Hrsg. von U. P. Kanning. 2007, S. 12–38, S. 14.

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 3.2 zeigt den Zusammenhang zwischen Kompetenz und Verhalten, der nach Kannung71 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, dass 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. 3.1 zeigt die Wissentreppe[72] von North[73], in der die Stufen einer kompetenten Handlung gezeigt werden. Die ersten vier 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 umgesetzt 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, dass 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[74]:

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

Sozialkompetenzen: kommunikatives und kooperatives Handeln, gruppen- und beziehungsorientiertes Verhalten, Entwicklung neuer Pläne, Werthaltungen und Ziele;

71 Kanning, s. Anm. 14.

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

73 K. North. Wissensorientierte Unternehmensführung. Wertschöpfung durch Wissen. 2., aktualisierte und erw. Aufl. 2002.

74 nach J. Erpenbeck und L. von Rosenstiel, Hrsg. Handbuch Kompetenzmessung. Erkennen, verstehen und bewerten von Kompetenzen in der betrieblichen, pädagogischen und psychologischen Praxis. 2., überarb. und erw. Aufl. 2007, S. XXIV.

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.

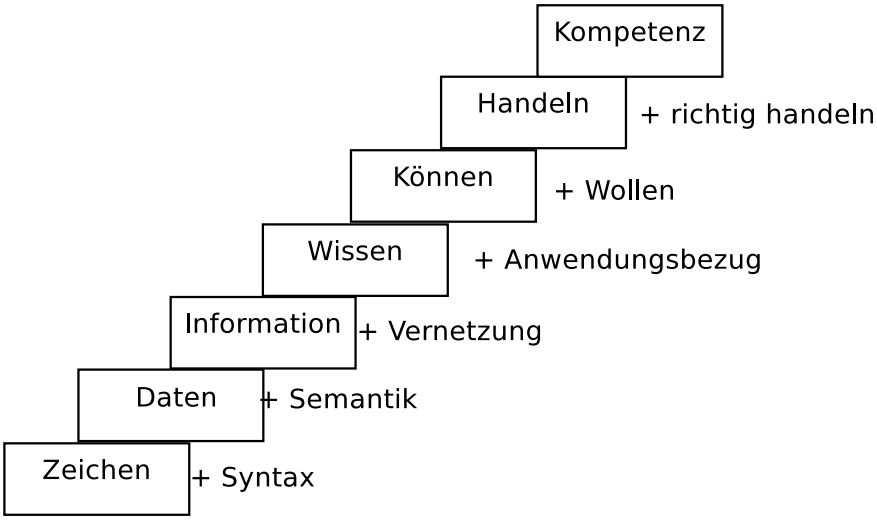


Abbildung 3.1: Wissenstreppe nach[75]; selbsterstellte, gekürzte Darstellung

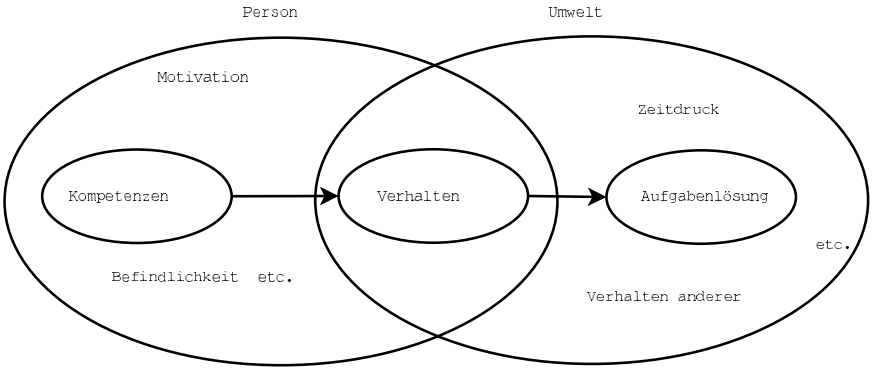


Abbildung 3.2: Zusammenhang zwischen Kompetenz und Verhalten, selbst erstellt nach[76]

Zeigt ein Individuum in allen vier Dimensionen kompetentes Verhalten, kommt es zur sogenannten Handlungskompetenz. Das Sekretariat der Kultusministerkonfe-

75 K. North. Wissensorientierte Unternehmensführung. Wertschöpfung durch Wissen. 2., aktualisierte und erw. Aufl. 2002.

76 Kanning, s. Anm. 14

renz[77] 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.

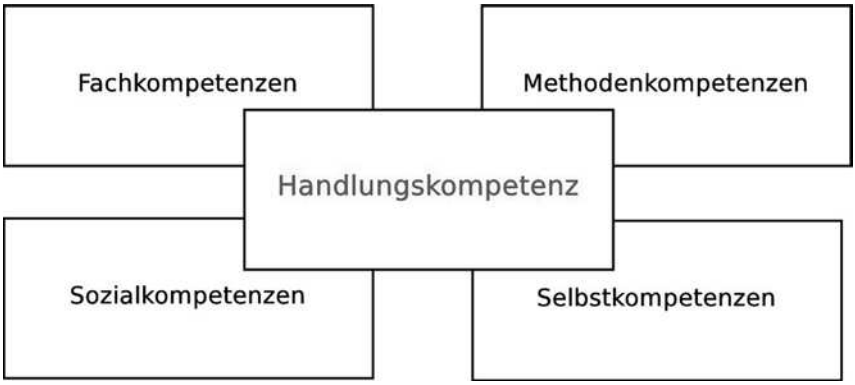


Abbildung 3.3: Grafische Darstellung der Kompetenzklassen, selbst erstellt

Das Kompetenzmodell wird zurzeit sowohl in der Berufspädagogik[78], in der Grundschulpädagogik[79] als auch in der Arbeitspsychologie und Eignungsdiagnostik80 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[81] für spezifische Fragestellungen, zum Beispiel die Ausprägung einzelner

77 Sekretariat der Kultusministerkonferenz, Hrsg. 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. http://www.kmk.org/fileadmin/veroeffentlichungen_beschluesse/2007/2007_09_01-Handreich-Rlpl-Berufsschule.pdf (besucht am 22. 04. 2009).

78 vgl. ebd.

79 vgl. Landesinstitut für Schule und Medien Berlin-Brandenburg, Hrsg. Kompetenzraster im Mathematikunterricht der Grundschule. 2007. http://bildungsserver.berlin-brandenburg.de/fileadmin/bbb/unterricht/faecher/naturwissenschaften/mathematik/Begleitheft_Kompetenzraster.pdf (besucht am 22. 04. 2009).

80 vgl. T. A. Langens, K. Sokolowski und H.-D. Schmalt. „Das Multi-Motiv-Gitter (MMG)“. In: Handbuch Kompetenzmessung. Hrsg. von J. Erpenbeck und L. von Rosenstiel. 2003, S. 71 - 79.

81 Ebd.

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.

3.2.1 Sicherheitskompetenz

Im vorhergehenden Kapitel habe ich gezeigt, dass Sicherheitskompetenz einen Bewertungsrahmen benötigt, um gemessen werden zu können. Dieser Bewertungsrahmen lässt sich 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[82].
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[83].
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 zehn Zeichen lang zu sein und je mindestens zwei Groß- und Kleinbuchstaben, zwei Sonderzeichen und zwei Ziffern zu enthalten, außerdem ist es geheim zu halten. 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 , wenn Alice ihr Passwort geheim hält 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"

82 vgl. v. a. Hacker, s. Anm. 5.

83 vgl. von Foerster, „Ethik und Kybernetik zweiter Ordnung", s. Anm. 24.

und „Gefechten“ auf operativer und taktischer Ebene[84]. 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 3.1) 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, dass nicht einmal nach Alice` vollendeter Handlung diagnostiziert werden kann, ob diese Handlung sicherheitskompetent war, da der Erfolg des Angriffs nicht nur von Alice´ Handlungen abhängt, sondern eben auch von anderen Organisationsmitgliedern, die angegriffen werden.

Satz 11 (determinierte kompetente Handlung)
Ist das Ergebnis einer kompetenten Handlung bekannt, heiße sie determinierte kompetente Handlung.

Satz 12 (nicht-determinierte kompetente Handlung)
Ist das Ergebnis einer kompetenten Handlung nicht bekannt, heiße sie nicht-determinierte kompetente Handlung.

4 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[85]. 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[86]. Auch im Falle der IT-Sicherheit gewinnt die Organisation bedeutenden Einfluss: sei es durch ihr formales Organisations-

84 C. von Clausewitz. Vom Kriege. 1832

85 vgl. N. Luhmann. Einführung in die Systemtheorie. Hrsg. von D. Baecker. 4. Aufl.. 2008; H. von Foerster. „Über selbstorganisierende Systeme und ihre Umwelten“. In: Wissen und Gewissen. Versuch einer Brücke. Hrsg. von S. J. Schmidt. 1993, S. 211–232; Maturana und Varela, Autopoiesis and Cognition, s. Anm. 29; Baecker, s. Anm. 25.

86 vgl. E. Witte. Organisation für Innovationsentscheidungen - Das Promotoren-Modell. 1973; Weber, „Wirtschaft und Gesellschaft“, s. Anm. 35; Weber, „Wirtschaft und Gesellschaft“, s. Anm. 35; K. Sonntag, Hrsg. Personalentwicklung in Organisationen. 2006; T. Brandenburg und T. Faber. „Fehlermanagement-Training Entwicklung sozialer Kompetenzen und der Umgang mit Fehlern in Risiko-Arbeitsbereichen“. In: Förderung sozialer Kompetenzen in der Personalentwicklung. Hrsg. von U. P. Kanning. 2007, S. 216–237.

modell[87], der Organisations- und Professionskultur[88], Kommunikationsdynamiken[89], Lernbarrieren[90], Lernkultur[91], die Konstruktion der Wirklichkeit[92] oder schlussendlich der „Vorwegnahme von Entscheidungen“[93]. 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[94] verweisen. Das zweite Problem, das der Organisation als Angriffsziel, möchte ich im folgenden anhand des historischen Verteidigungskonzeptes „Verteidigung in der Tiefe“ illustrieren.

4.1 Verteidigung in der Tiefe

Verteidigung in der Tiefe ist ein Verteidigungskonzept, das 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[95]. Abb. 4.1 zeigt die

87 vgl. F. X. Bea und E. Göbel. Organisation. Theorie und Gestaltung. 3., neu bearbeitete Auflage. 2002.

88 vgl. B. Schmid und A. Messmer. Systemische Personal-, Organisations- und Kulturentwicklung. Konzepte und Perspektiven. 2005.

89 vgl. G. Mohr. Systemische Organisationsanalyse. Dynamiken und Grundlagen der Organisationsentwicklung. 2006.

90 vgl. J. Schüppel. Wissensmanagement. Organisatorisches Lernen im Spannungsfeld von Wissens- und Lernbarrieren. 1999.

91 vgl. H. Willke. Systemisches Wissensmanagement. 2., neubearb. A. 2001.

92 vgl. P. L. Berger und T. Luckmann. Die gesellschaftliche Konstruktion der Wirklichkeit. Eine Theorie der Wissenssoziologie. 20. Aufl. 2004.

93 vgl. Baecker, „Zum Problem des Wissens in Organisationen“, s. Anm. 39.

94 vgl. Sonntag, s. Anm. 2.

95 vgl. A. Zinsmeister. „Abwehr. Urbane Topographien“. In: Abwehr. Hrsg. von C. Pias. 2009, S. 147–168; Die Verteidigung in der Tiefe angewandt auf IT-Systeme (Memento). In: (2004). Hrsg. von Secrétariat général de la défense nationale. http://www.ssi.gouv.fr/de/vertrauen/documents/methods/

Festung Magdeburg um 1750. Die „Zacken“ um die Stadtmauer 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 „Abwehr. Modelle Strategien Medien“[96] diskutiert, vor allem auch in „Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit“[97].

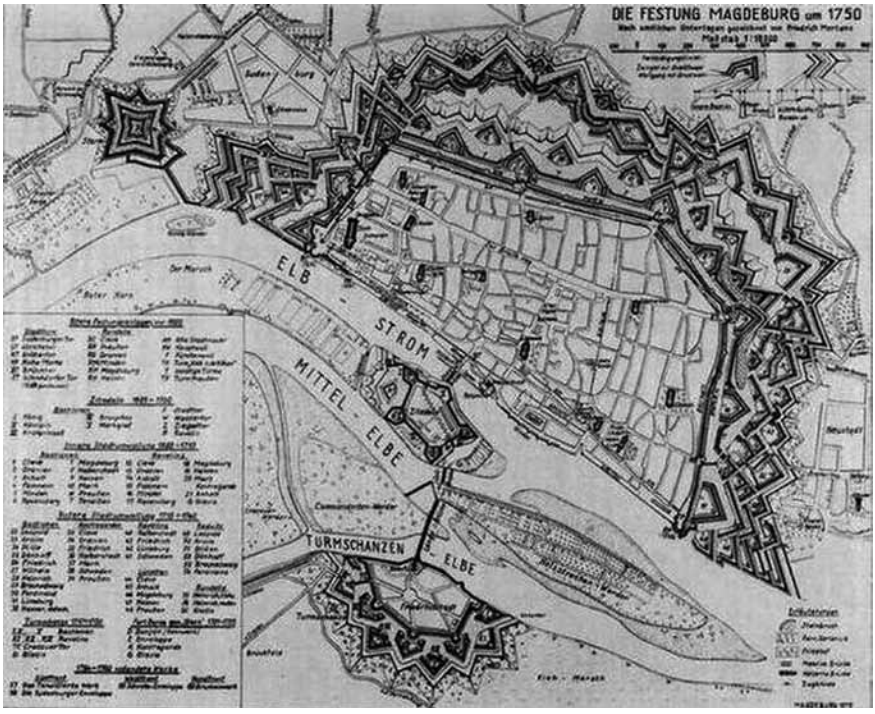


Abbildung 4.1: Die Festung Magdeburg um 1750

Das Konzept der Verteidigung in der Tiefe wird schon seit einigen Jahren, wenn nicht gar Jahrzehnten, in der IT-Sicherheit angewandt und „gepredigt“[98, 99]. 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. 4.2). Es können auch mehrere gestaffelte Sicherheitsmechanismen eingesetzt werden, wie Paketfilter, verschlüsselnde Dateisysteme, Intrusion Detection Systeme und Honeypots, Datensicherung und -vernichtung oder Steuerung der Systemcalls[100].

mementodep-V1.1_de.pdf (besucht am 25. 10. 2006).

96 C. Pias, Hrsg. Abwehr. Modelle Strategien Medien. 2009.

97 Zinsmeister, s. Anm. 11.

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

99 vgl. Secrétariat général de la défense nationale, s. Anm. 11.

100 vgl. S. Schumacher. Methoden zur Datensicherung Strategien und Techniken für NetBSD. 2006. http://www.net-tex.de/backup.pdf; S. Schumacher. Methoden zur Datensicherung Strategien und

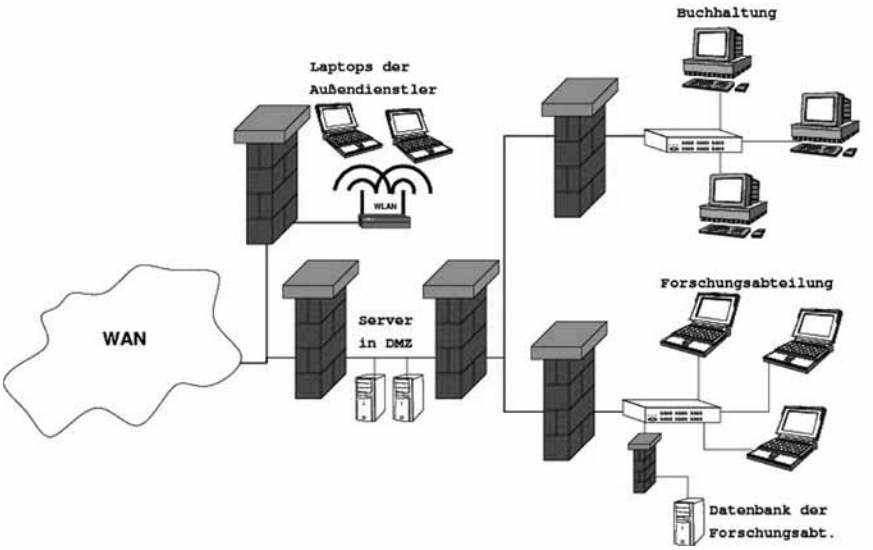


Abbildung 4.2: Verteidigung in der Tiefe durch Netzsegmentierung mittels Firewall

Die Verteidigung in der Tiefe muss aber nicht nur in der technischen Dimension ausgerollt werden, sondern auch in der sozialen und technisch-sozialen Dimension (Satz 2). Bisher etablierte Beispiele sind die physikalische Sicherung von Computern in speziell geschützten Räumen mit Zugangsbeschränkung 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 Alice´ 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

Techniken für NetBSD . In: Proceedings des GUUG Frühjahrsfachgespräches 2006. (Universität Osnabrück). Hrsg. von German Unix User Group. Berlin: Lehmanns Media, 2006, S. 79-98; Schumacher, „Auf dem Weg zum Intrusion Detection System der nächsten Generation", s. Anm. 14; S. Schumacher. „Verschlüsselte Dateisysteme für NetBSD". In: UpTimes 4 (2006), S. 25–31. http://kaishakunin.com/publ/guug-uptimes-cgd_cfs.pdf (besucht am 07. 11. 2009); S. Schumacher. „Sicherung verteilter Systeme mit Bacula". In: UpTimes 4 (2006), S. 14–20. http://kaishakunin.com/publ/guug-uptimes- bacula.pdf (besucht am 07. 11. 2009); S. Schumacher. „Daten sicher löschen". In: UpTimes 1 (2007), S. 7–16.

beeinflusst[101] 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 umfassen, 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 Biologie102 und Entwicklungspsychologie (vgl. R. Brooks und S. Goldstein. Das Resilienz-Buch. Wie Eltern ihre Kinder fürs Leben stärken, das Geheimnis der inneren Widerstandskraft. 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[103], armen Familien[104] oder traumatisierten Adoptivkindern[105]. Ich möchte daher dieses Konzept, das auch eng mit der Idee der Lernenden Organisation verwandt ist[106], wie folgt definieren:

Satz 13 (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 14 (Resiliente Organisation)
Eine Organisation ist resilient, wenn sie auch bisher unbekannte Angriff erkennt und auf diese reagieren kann. Eine Resiliente Organisation ist zwingend fähig zur Erkenntnis und zu kompetentem Handeln.

101 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.

102 B. Walker und D. Salt. Resilience thinking: sustaining ecosystems and people in a changing world. 2006

103 vgl. D. W. Haines, Hrsg. Refugees as Immigrants. Cambodians, Laotians and Vietnamese in America. 1989.

104 vgl. „Arme Familien gut beraten. Hilfe und Unterstützung für Kinder und Eltern". In: (2004). Hrsg. von Bundeskonferenz für Erziehungsberatung e.V. http://www.bke.de/content/application/shop.download/1257417004_Arme%20familien%20PM%2072.pdf (besucht am 05. 01. 2011).

105 vgl. D. Thränhardt und U. Hunger. Einwanderer-Netzwerke und ihre Integrationsqualität in Deutschland und Israel. Studies in migration and minorities. 2000.

106 vgl. P. Senge und M. Klostermann. Die fünfte Disziplin: Kunst und Praxis der lernenden Organisation. 2008.

Erst auf organisationaler Ebene ist es also möglich, auf alle möglichen, auch unbekannten, Angriff 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 identifizieren und selbständig neuartige Abwehrmethoden zu etablieren[107]. Daher ist es im weiteren notwendig, Erkenntnisfähigkeit als Grundlage einer Lernenden Organisation zu untersuchen und Personal und Organisationskonzepte zu entwerfen, die in Anlehnung an Senge und Klostermann[108] zu Erkenntnisfähigkeit und selbständigem Handeln auf allen Ebenen führen.

5 Fazit

Im Rahmen dieser Arbeit habe ich gezeigt, dass eine rein technische Betrachtung der Sicherheit von IT-Systemen bei weitem nicht ausreicht. Ich habe gezeigt, dass sich die IT-Sicherheit in die technische, psychische und soziale Dimension erstreckt und dort mit den jeweils geeigneten Methoden untersucht werden muss. Ich habe außerdem gezeigt, dass die soziale und die psychische Dimension die technische determinieren können, dass dies umgekehrt aber sehr schwer möglich ist. In der Praxis heißt das, dass Computerprogramme nur in einem sehr engen Rahmen Sicherheit herstellen können. Im Gegenzug bieten Personal- und Organisationsentwicklungsmaßnahmen ausreichend Potenzial und Spielraum, um effektiv und effizient auf die Sicherheit eines IT-Systems einzuwirken.

Hier bieten Kompetenzmodelle und deren Anwendung zur Diagnose und Entwicklung von menschlichen Handlungen exzellent geeignete Werkzeuge. Diese müssen in weiteren Arbeiten auf den Bereich IT-Sicherheit und Organisationssicherheit übertragen werden. Dazu kann beispielsweise auf die Förderung Sozialer Kompetenzen oder Risiko- und Fehlermanagement bzw. Arbeiten aus dem Bereich Luft und Raumfahrt und Arbeitsprozesse in Kernkraftwerken zurückgegriffen werden. Desweiteren wird in der Organisationsentwicklung bzw. im Wissensmanagement der Einfluss der Organisation auf die Personalentwicklung ausführlich diskutiert, so dass dieser Bereich ebenfalls für die Organisationssicherheit fruchtbar gemacht werden kann. Besonderes Augenmerk gilt hierbei dem nicht-determinierten, sicherheitskompetenten Verhalten, da hierbei der Organisation besondere Bedeutung beikommt. Schließlich ist es nur auf der Ebene der Organisation möglich, bestimmte Angriffe auf die Sicherheit eines Systems zu erkennen und dagegen vorzugehen. Daher sind meine Ansätze zur Resilienz einer Organisation weiter auszubauen. Nach einer adäquaten (und umfangreichen) Diskussion des Resilienz-Begriffes kann dieser angewandt werden, um Organisationstheorien auf ihre Anwendbarkeit bezüglich Sicherheit zu untersuchen. Es ist außerdem notwendig, die Diskussion um den Begriff der IT-Sicherheit, dessen Definition bzw. Explikation und seine praktische Anwendbarkeit wei-

107 Die Diagnostik von Sicherheitsvorfällen und die dazu notwendige Erkenntnisfähigkeit habe ich in Schumacher, „Auf dem Weg zum Intrusion Detection System der nächsten Generation“, s. Anm. 14 diskutiert.

108 Senge und Klostermann, s. Anm. 22; C. O. Scharmer. Theory U. Leading from the Future as it Emerges. 2007.

ter zu führen. Dabei ist darauf zu achten, dass der Beobachter[109], also der Mensch, nicht ausgeschlossen wird. Schlussendlich muss eine eigenständige Disziplin der Sicherheitsforschung etabliert werden. Weder die Ingenieurwissenschaften, noch die Erziehungswissenschaft, Psychologie oder Soziologie sind für sich genommen in der Lage, die Phänomene vollständig zu bearbeiten. Als Beispiel kann hier die Ingenieurspsychologie dienen, die sich unter anderem mit der Kommunikation in Mensch-Maschine-Systemen, der psychischen Regulation von Arbeit oder der Usability befasst. Diese Bereich sind aber noch nicht ausreichen, da unter Umständen eigene Forschungsmethoden ebenso entwickelt werden müssen wie Kompetenzmodelle oder Kompetenzentwicklungsverfahren sowie eine eigenständige Fachdidaktik. Bei all diesen psychischen und sozialen Bereichen darf die technische Seite nicht ausgeschlossen oder marginalisiert werden, daher kann nur ein interdisziplinärer Ansatz Erfolg versprechen.
Ich hoffe mit dieser Arbeit einen ersten Schritt in die Richtung einer eigenständigen Sicherheitsforschung getan zu haben.

109 "Anything said is said by an observer. In his discourse the observer speaks to another observer, who could be himself; whatever applies to the one applies to the other as well. The observer is a human being, that is a living system, and whatever applies to living systems applies also to him." Maturana und Varela, Autopoiesis and Cognition, s. Anm. 29