Auf dem Weg zum Intrusion Detection System der nächsten Generation

Stefan Schumacher
Stefan.Schumacher@Kaishakunin.com
http://www.Kaishakunin.com

Kaishakunin.com
Agentur für Unternehmenssicherheit
Weinbergstrasse 1
39106 Magdeburg

Zusammenfassung

Auf den Chemnitzer Linux-Tagen 2005 habe ich in meinem Vortrag »Einbruchserkennung in Netzwerke mit Intrusion Detection Systemen« die Funktionsweise von IDS beschrieben. In den letzten Jahren hat sich der Hype um Snort &. Co. etwas gelegt und die systembedingten Grenzen wurden aufgezeigt. So sind IDS immer noch nicht in der Lage, unbekannte Angriffe zu erkennen oder gar das soziale System einer Organisation zu analysieren.

Ich zeige anhand von Beiträgen aus der Philosophie, Pädagogik und Psychologie, wie Erkenntnis und Lernen funktioniert und welche Voraussetzungen erfüllt sein müssen, um lernende und erkennende IDS aufzubauen.

1 vom zwecke dieses werkes

Intrusion Detection Systeme (IDS) dienen dazu, Einbrüche bzw. Einbruchsversuche in Netzwerke zu entdecken und zu unterbinden. Dazu überwachen Sie im Normalfall den Netzwerkverkehr anhand verschiedener Monitor in Netzwerk, führen die gesammelten Daten auf einem Server zusammen und vergleichen diese mit einem Einbruchslexikon, in dem Signaturen für Einbrüche gesammelt sind. Treffen sie einen Lexikoneintrag, geben sie Alarm oder lösen eine sonstige Präventivmaßnahme aus.

Sie ergänzen damit als Teil des Sicherheitskonzeptes andere technische Sicherheitsstrategien wie Zugangsschutz, Identifikation, Autorisierung, Datensicherung und soziale Maßnahmen (Vorschriften, Policies, Verträge ...).

Die Einbruchserkennung ist notwendig bzw. sinnvoll, da in der Regel die einzelnen Maßnahmen die Sicherheit einer Organisation nicht komplett gewährleisten können bzw. nicht alle Angriffsszenarien abdecken oder gar selbst angegriffen und ausgehebelt werden können.

Das IDS ist somit ein Baustein der Sicherheitsstrategie und Teil der gestaffelten Verteidigung in der Tiefe »des Raumes« (vgl. Clausewitz 1832; Secrétariat général de la défense nationale 2004).

Da ein Einbruch aber nicht nur aus TCP/IP-Paketen besteht, sondern oftmals auch auf einer sozialen Ebene wie z. B. Social Engineering, (vgl. Kehrer 2008; N.N. 2009; Schumacher 2009*a*,*b*,*c*,*d*) stattfindet, ist es zwingend erforderlich diese Ebene ebenfalls zu analysieren.

Darüberhinaus sind die gegenwärtigen IDS nicht in der Lage neuartige Angriffe zu erkennen. Sie verwenden im Prinzip Lexika, in denen bereits erkannte und analysierte Angriffe aufbereitet wurden und vergleichen diese mit dem Netzwerkverkehr. Sie basieren daher auf einem Regelsystem, das ein Angreifer nur auszuhebeln oder zu umgehen braucht, um einen erfolgreichen Angriff durchzuführen.

Daher ist es notwendig, IDS zu entwickeln, die *erkennen* können, also erkenntnisfähig sind. Erkenntnis lässt sich als durch Erfahrung gewonnene Einsicht beschreiben. Kant unterschied Erkenntnis nach der Art der Gewinnung in a priori und posteriori. A priori meint dabei die von der Erfahrung unabhängige Erkenntnis, die allein mit den Mitteln der Vernunft begründet werden kann. A posteriori bezeichnet die Erkenntnis aus Erfahrung (vgl. Poser 2001, S. 32). Dazu gehört die Fähigkeit, eine Diagnose zu stellen, also die »Merkmale eines Sachverhaltes zu erfassen« und daraus eine Prognose, also »die Vorhersage eines Ereignisses aufgrund vorliegender Begebenheiten« abzuleiten (Schnotz 2006, S. 8; zitiert nach Fuhrer 2009). Dabei ist es zur Abwehr ausgefeilter Attacken notwendig, Menschliches Verhalten und soziale Beziehungen zu analysieren.

Das heißt, ein erkennendes IDS soll in der Lage sein aus Erfahrungen neue Einsichten zu generieren und diese bspw. in neue Sicherheitsregeln umzusetzen.

2 vom zeichen über das wissen zur handlung

Um erkenntnisfähig sein zu können, benötigt ein IDS eine kybernetische Rückkopplungsschleife. Das heißt, das System, muss über ein Wahrnehmungsorgan verfügen, das Reize aus der Umwelt aufnimmt und diese Reize im System weiterverarbeitet. Aufgrund des Ergebnisses der Verarbeitung nimmt das System eine Anpassung des eigenen Verhaltens vor (vgl. v. a. Kap. »Kybernetik einer Erkenntnistheorie« Foerster 1993).

Stark vereinfacht muss ein erkennendes bzw. lernfähiges IDS dazu »nur« folgende Schritte durchführen:

1. Das System muss seine Umwelt wahrnehmen.
2. Die wahrgenommene Umwelt muss verarbeitet werden (Diagnose), dazu muss Wissen bzw. Erfahrung über stattgefundene Sicherheitsvorfälle (post mortem) aufgebaut werden.
3. Mit der aktuell wahrgenommenen Umwelt kann anhand des erstellen Erfahrungsrahmen ein Sicherheitsvorfall, der erst noch stattfinden wird, prognostiziert werden.

North (2002) beschreibt in seiner Wissenstreppe (Abb. 1), wie Wissensmanagement und damit Wissen aufgebaut wird. Zeichen werden mit einer Syntax zu Daten, Daten mit einer Semantik zu Information, Information mit Vernetzung zu Wissen und Wissen mit Anwendungsbezug zu Können.

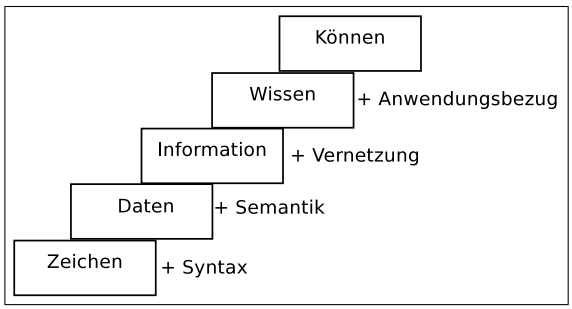

Abbildung 1: Wissenstreppe nach North (2002); angepasste, gekürzte Darstellung

Nimmt man dieses (angepasste) Modell als Grundlage für die Entstehung von Handlungskompetenz, muss ein erkennendes IDS folgende Handlungen ausführen können:

1. Weltwahrnehmung: das IDS muss in der Lage sein, Reize aus der Umwelt aufzunehmen und zu *verarbeiten*. Die aufgenommenen Reize können als Zeichen im Sinne der o.g. Wissenstreppe betrachtet werden.
2. Ordnung: Die wahrgenommenen Zeichen müssen eingeordnet werden, es muss eine Syntax generiert werden. Diese Ordnung ist für alle Reize bzw. Zeichen notwendig. Dies ist einfach für die Zeichen formaler Sprachen (z. B. Quellcode, Maschinencode, TCP/IP-Pakete, ZIP-Archive, MP3-Dateien) aber kaum lösbar für natürliche »Sprachen«, wie dem Verhalten von Menschen.
3. Die nun gewonnen Daten müssen eine Semantik d. h. eine *Bedeutung* erhalten. Somit werden aus Daten Informationen.
4. Informationen müssen vernetzt werden. Ähnlich wie man Buchstaben zu Wörtern, Wörter zu Sätzen und Sätze zu Büchern verknüpft, muss ein semantisches Netz zwischen den einzelnen Daten aufgespannt werden. Die Daten als Atome des Wissens müssen über Relationen miteinander verknüpft werden. Somit entsteht Wissen.
5. Das nun vorhandene Wissen muss in einen Anwendungsbezug, einen Kontext gestellt werden. Ein in Schritt 1 wahrgenommenes Zeichen existiert nicht für sich allein und kann somit auch nicht isoliert betrachtet werden, vielmehr wurde es innerhalb eines Handlungsrahmens erzeugt und muss auch in diesem Handlungsrahmen interpretiert werden. Die Interpretation unterliegt dabei der Kybernetik zweiter Ordnung (vgl. Foerster 2008).

2.1 *Grundsätzliche diagnostische Probleme*

Unabhängig davon wer (oder was) die Umwelt analysiert um Prognosen über Sicherheitsvorfälle abzugeben, wird immer wieder auf einige systemimmanente diagnostische Probleme stoßen.

Prinzipiell funktioniert eine Prognose so, das zum Zeitpunkt t_0 vorhergesagt werden soll, ob es zum Zeitpunkt $t_{>0}$ zu einem Sicherheitsvorfall kommen wird. Dazu stehen nur alle bis zu t_0 gesammelten Daten und bis dahin aufgebauten Erfahrungen zur Verfügung.

Damit zeigen sich bereits zwei potentielle Fehlerquellen auf: die gesammelten Daten und der zu erstellende Erfahrungsrahmen.

Die zu sammelnden Daten müssen die gesamte Organisation umspannen und zentral verarbeitet werden. Das bedeutet, das im Prinzip alles was innerhalb der Organisation stattfindet überwacht und ausgewertet werden muss. Ein Angriff kann schließlich an verschiedenen Orten stattfinden bzw. dort vorbereitet werden. Problematisch ist hierbei zum einen die Möglichkeit Daten überhaupt zu sammeln. Man kann zwar technisch alle Telefonate und E-Mails mitschneiden, diese aber nur schwer automatisch auf ihren Sinn hin interpretieren lassen. Ebenso verhält es sich mit der sozialen Ebene. War der nette Herr Dr. Müller-Lüdenscheid, der heute Morgen am Empfang Fragen stellte wirklich ein potentieller Kunde, oder wollte er nur Informationen für eine Social-Engineering-Attacke sammeln? Es wäre zwar hier auch technisch möglich mittels

Kamera und Mikrofon das Gespräch aufzuzeichnen, es ist aber nicht möglich es automatisch auszuwerten, von datenschutzrechtlichen Bedenken einmal ganz abgesehen.

Außerdem droht das Problem, in den gesammelten Daten zu ertrinken, d. h. die reine Datenmenge steigt derart an, das sie nicht mehr oder zumindest nicht mehr zeitnah zu verarbeiten ist.

Der Erfahrungsrahmen ist eine weitere Problemquelle. Selbst wenn wir annehmen, dass alle Daten, die zu einem erfolgten Angriff gehören erfasst wurden, bedeutet dies noch lange nicht, das wir sie im Erfahrungsrahmen verarbeiten können.

Zum einen ist hier die *Qualität* der Daten ein Problem: Schließlich können wir nur solche Sicherheitsvorfälle post-mortem analysieren, die uns überhaupt erst einmal aufgefallen sind. Das wiederum bedeutet aber, das unsere Datenbasis aus Daten gescheiterter Einbrüche – also minderer Qualität – besteht. Die Daten wirklich erfolgreicher Einbrüche können wir nicht analysieren, da wir von einem erfolgreichen Einbruch schlichtweg nichts wissen.

Weiterhin kommt es bei der Erstellung des Erklärungsrahmens auf die Biographie des »Erklärers« an. Bereits gemachte Erfahrungen beeinflussen sein Weltbild, somit auch neue, noch zu machende Erklärungen. Das heißt, das zwei unterschiedliche IDS unterschiedliche Erklärungen für Daten finden können. Dies wird insbesondere von Heinz von Foerster unter dem Stichwort Kybernetik zweiter Ordnung ausgiebig diskutiert, vgl. hierzu vor allem Foerster (2008); Foerster und Pörksen (2006), dies würde hier aber den Rahmen des Beitrages sprengen.

3 PIAGETS GENETISCHE EPISTEMOLOGIE

Der schweizer Biologe Jean Piaget (1896 – 1980) war Zeit seines Lebens daran interessiert, wie Menschen Erkenntnis aufbauen. Dazu untersuchte er Kinder und ihre ihre Entwicklungsschritte. Auf Grundlage dieser Beobachtungen erschuf er seine Theorie der »genetischen Epistemologie[1]« und der Entwicklungsstufen des Menschen, die hier aber nicht Bestandteil der Betrachtung sind.

Diese Theorie der genetischen Epistemologie beschreibt, wie Menschen ihren Erkenntnisapparat aufbauen und wie Erkenntnis im menschlichen Geist entsteht. Daher eignet sie sich als Entwurfsreferenz für ein erkennendes IDS und soll hier exemplarisch für eine Theorie der Erkenntnis vorgestellt werden.

Darwin führte in seinen Werken das Konzept der Entwicklung als Evolution bzw. Epigenese ein, d. h. es entstehen im Organismus neue Strukturen, die nicht bereits im Ei bzw. dem Samen angelegt waren. Evolution ist demnach ein Prozess, der *neue* Strukturen und Eigenschaften des Organismus – und damit Fähigkeiten – aus seinen Genen entwickelt. Dabei hat die Evolution keinen bestimmbaren Beginn und kein bestimmbares Ende.

Der zentrale theoretische Begriff der genetischen Epistemologie ist die Struktur als richtungsweisender Kern der Entwicklung. Der Begriff Struktur wurde vom Konzept des biologischen Holismus (Ganzheitslehre).

Strukturen beschreiben Wahrnehmung über allgemeine Formen und Erkenntnis über ihr internes Schema. Strukturen beschreiben damit, wie Wahrnehmnung aufgebaut ist. Piaget beschreibt den menschlichen Geist als Organismus, welcher von seiner Umwelt unterschieden werden kann, aber mit ihr interagiert. Allgemein sind Strukturen Systeme von Beziehungen zwischen ihren Elementen und zwischen den Elementen und dem Ganzen. Diese Systeme sind nicht-statisch und selbstorganisierend, das Ganze ergibt somit mehr als die Summe seiner Teile, ebenso wie Wahrnehmung mehr ist als die Summe empfundener Reize. Jede Struktur ist dabei das Moment einer unabgeschlossenen *und* unabschließbaren Entwicklung. Der Vorteil einer Struktur ist, das sie dabei auf Denken *und* Welt, Geist *und* Materie angewendet werden kann.

Nachdem ich nun dargelegt habe, wie in der genetischen Epistemologie Strukturen die Grundlage der Theorie bilden, stellt sich die Frage, wie Strukturen erzeugt bzw. angepasst werden.

Piaget geht davon aus, das die Basisstrukturen im Menschen durch biologische »Hardware« bereitgestellt werden, bspw. das visuelle System mit Auge und Retina, Sehnerv, ventraler und dorsaler Pfad, Teile des Thalamus, des Hirnstamms sowie der Sehrinde (vgl. Pollmann 2008, Kap. Wahrnehmung). Diese Struktur ermöglicht es uns zu sehen und visuell wahrzunehmen. Ähnlich stellt die Hardware eines Computer Grundstrukturen bereit, bspw. über das BIOS und die CPU entsprechende Rechenwerke, I/O-Befehle usw. Diese biologischen bzw. hardwareseitigen Strukturen ermöglichen den Aufbau weiterer Strukturen, bspw. das Lesen oder eine TCP/IP-Schnittstelle.

Strukturen werden aufgebaut bzw. aktualisiert, in dem Objekte in Strukturen assimiliert werden und Strukturen durch Objekte akkommodiert werden. Assimilation heißt, das subjektive Strukturen auf Objekte angewandt werden, um diese Objekte in die Struktur einzupassen, also zu assimilieren. Akkomodation bedeutet, das ein Objekt die Struktur anpasst:

> Allgemein können Strukturen als Systeme von Wechselbeziehungen unter ihren Elementen sowie zwischen diesen Elementen und dem Ganzen definiert werden. Nach Piaget sind dabei drei

[1] Erkenntnistheorie

> Merkmale notwendig: »Eine Struktur besitzt erstens Totalitätsgesetze, die andere sind als die ihrer Elemente und die es sogar ermöglichen, von derartigen Elementen ganz abzusehen. Zweitens sind diese Eigenschaften der Gesamtheit Transformationsgesetze. ... Drittens beinhaltet jede Struktur eine Selbstregelung im zweifachen Sinn. Ihr Aufbau führt niemals über ihre Grenzen hinaus und benötigt niemals etwas von außerhalb dieser Grenzen.«

(Scharlau 2007, S. 84)

Ein Kind lernt beispielsweise, das ein Dackel ein Element der Klasse »Hund« ist. Es abstrahiert aus den Eigenschaften des Dackels Eigenschaften für die Klasse »Hund«, bspw. klein, 4 Beine, wedelnder Schwanz, kurzes, braunes Fell. Später sieht es einen Deutschen Schäferhund und erfährt, das dies auch ein »Hund« ist. Der Deutsche Schäferhund wird also in die Struktur Hund assimiliert. Gleichzeitig akkommodiert der Schäferhund aber die Struktur Hund, da die Eigenschaft »klein« nicht auf ihn zutrifft.

Dieses Beispiel zeigt auch, das Assimilation und Akkommodation nicht exklusiv, sondern immer zusammen auftreten. Ein Objekt wirkt also immer assimilierend und akkommodierend zugleich. Wahrnehmung organisiert damit externe Ereignisse und Objekte mit Hilfe existierender Wahrnehmungsstrukturen.

Ein maßgeblicher Punkt jeder Lerntheorie ist die Frage nach der Lernmotivation: Warum will jemand lernen bzw. warum wird überhaupt gelernt? Piaget selbst entwickelte keine explizite Motivationstheorie. Stattdessen beschrieb er die Strukturen als äquilibriert, d. h. als im Gleichgewicht befindlich. Sind die Strukturen im Gleichgewicht, sind sie stabil und unanfällig gegen Fehler. Wird nun ein Reiz aus der Umwelt wahrgenommen, der nicht mit den aufgebauten Strukturen übereinstimmt, geraten diese aus dem Gleichgewicht und müssen aktualisiert werden, entweder durch assimilieren oder akkommodieren. Jede höhere Struktur wird damit umfangreicher als ihre Vorgänger. Im o. g. Beispiel stört die Information das der Schäferhund groß ist, die Eigenschaft »Hunde sind klein«. Daher muss das Kind die Struktur »Hund« akkommodieren und die Größeneigenschaften anpassen.

Piaget betont aber auch, das Erkenntnis mehr ist, als nur das Sammeln von Daten. Stattdessen würden reflektierende Abstraktionen notwendig sein, in der Menschen über ihre Strukturen reflektieren, und wie diese alten Strukturen die Entstehung neuer Strukturen beeinflussen:

> Erkenntnis ist aber mehr als Anhäufung von Tatsachen, und zwar aktive theoretische Verknüpfung und Interpretation dieser Tatsachen. Dem trägt die reflektierende Abstraktion (oder logisch-mathematische Erfahrung) Rechnung. Sie abstrahiert nicht von Objekten, sondern von Operationen des Subjekts und hierbei wiederum besonders von deren Koordination, der Verbindung von Handlungen in Zeitverhältnissen, Mittel-Ziel-Beziehungen, Zuordnungen sowie logischen Klassen und Relationen.

(Scharlau 2007, S. 101f)

4 CODA

Sicherheitsvorfälle zu diagnostizieren ist schwer, sie zu prognostizieren ungleich schwerer. Im Rahmen meiner Forschung befasse ich mich seit einigen Jahren mit der Frage, ob Computer überhaupt in der Lage sind, Sicherheitsvorfälle zu untersuchen oder gar vorherzusagen. Unabhängig von den ungelösten – und meiner Meinung nach unlösbaren Problemen – dass Computer keine Entscheidungen treffen können und Sicherheit nicht deterministisch-determiniert ist ergeben sich aus den Forschungsansätzen noch ganz andere »Probleme«, die ich in einem kleinen Gedankenexperiment diskutieren möchte.

Angenommen es gäbe ein erkennendes IDS, welches ebenso intelligent wie ein Mensch sei, ergeben sich folgende Probleme:

- Intelligenz und Erkenntnisfähigkeit führen zumindest zu einer eingeschränkten Form der Identität. Das heißt, das ein IDS sich selbst erkennt, es also einen Begriff von sich selbst, ein »Ich« entwickelt. Das wiederum hat zur Folge, das es zielgerichtete Handlungen durchführen kann. Oder auch nicht, denn es kann nun wollen – oder eben nicht wollen.
- Jedes erkennende IDS wird einzigartig sein. Da das IDS erst in seiner Organisation lernt, entwickelt es sich unterschiedlich. Angenommen ich installiere zum 01.01 das selbe IDS an der Uni Magdeburg und der TU Chemnitz und lasse sie bis zum 31.12. laufen, dann haben beide IDS unterschiedliche Erfahrungen gemacht. Sie sind damit nicht mehr vergleichbar! Es kann sein, dass das IDS in Chemnitz einen Sicherheitsvorfall entdecken wird, den das IDS in Magdeburg nicht erkennt, und umgekehrt. Ebenso wie sich zwei Diplom-Informatiker unterscheiden werden, die in Magdeburg und Chemnitz studiert haben, werden sich die beiden IDS unterscheiden. Derartige Untersuchungen wurden in der Psychologie und angrenzenden Gebieten schon durchgeführt – an eineiigen Zwillingen (vgl. v. a. die Minnesota-Zwillingsstudie in Friedman und Schustack 2004).
- Aufgrund der Einzigartigkeit der IDS sind kompetenzdiagnostische Maßnahmen notwendig. Da sich wie oben beschrieben die IDS unterscheiden, sind sie auch unterschiedlich gut darin, Sicherheitsvorfälle festzustellen. Das wiederum führt dazu, dass wir feststellen müssen, welches IDS »besser« bzw.

»am besten« ist. Somit stehen wir wieder vor dem Problem, die Kompetenzen der IDS messen zu müssen, bspw. durch Bewerbungsgespräche, Assessment Center oder Arbeitsproben.

- Ein erkennendes IDS wird Fehler machen. Das heißt es wird einige Sicherheitsvorfälle nicht erkennen. Es wird falsch-positive und falsch-negative Alarme liefern und eine Erkennungsquote von weit unter 100% haben. Dies ist übrigens kein Problem der Intelligenz, sondern des Fehlers bzw. des naturalistischen Fehlschlusses und seines (mangelhaften) Bezugsrahmens. (vgl. Poser 2001)

5 ÜBER DEN AUTOR

Stefan Schumacher ist selbständiger Unternehmensberater (`Kaishakunin.com`) mit Schwerpunkt auf Unternehmenssicherheit, Social Engineering und Security Awareness. In seiner Freizeit studiert er Bildungswissenschaft und Psychologie in Magdeburg.

LITERATURVERZEICHNIS

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

Foerster, Heinz von (1993). *Wissen und Gewissen*. 1. Auflage. Frankfurt: Suhrkamp. 396 Seiten. ISBN: 978-3518284766.

– (2008). „Ethik und Kybernetik zweiter Ordnung". In: *Kurzzeittherapie und Wirklichkeit*. Herausgegeben von Paul Watzlawick und Giorgio Nardone. München: Piper, Seiten 71 – 89. ISBN: 9783492041126.

Foerster, Heinz von und Bernhard Pörksen (2006). *Wahrheit ist die Erfindung eines Lügners. Gespräche für Skeptiker*. 7. Auflage. Heidelberg: Carl-Auer-Systeme. 166 Seiten. ISBN: 9783896706461.

Friedman, Howard S. und Miriam W. Schustack (2004). *Persönlichkeitspsychologie und Differentielle Psychologie*. 2., aktualis. A. München: Pearson Studium. 768 Seiten. ISBN: 978-3827371058.

Fuhrer, Urs (2009). *Pädagogische Psychologie 1*. Unveröffentlichtes Skript zur Vorlesung im WS 2009/10. Otto-von-Guericke-Universität Magdeburg.

Kehrer, Anika (2008). „IT-Security psychologisch implementieren". In: *Linux-Magazin*. Bericht vom Frühjahrsfachgespräch 2008 über den Vortrag *Design und Implementierung einer Security-Awareness-Kampagne*. URL: `http://www.linux-magazin.de/NEWS/GUUG-Fachgespraech-IT-Security-psychologisch-implementieren` (besucht am 22. 10. 2009).

N.N. (2009). „Risiken durch Manipulation per Social-Engineering". In: *Entwickler Magazin* (2009. März 2009). Bericht vom Frühjahrsfachgespräch 2009 über den Vortrag *Psychologische Grundlagen des Social-Engineering*. URL: `http://entwickler.de/zonen/portale/psecom,id,99,news,47855,p,0.html` (besucht am 2009. 03. 20).

North, Klaus (2002). *Wissensorientierte Unternehmensführung. Wertschöpfung durch Wissen*. 2., aktualisierte und erw. Aufl. Wiesbaden: Gabler. 290 Seiten. ISBN: 978-3409230292.

Pollmann, Stefan (2008). *Allgemeine Psychologie*. 1. Auflage. München: UTB Reinhardt. ISBN: 97838252983919.

Poser, Hans (2001). *Wissenschaftstheorie*. 1. Auflage. Stuttgart: Reclam. 305 Seiten. ISBN: 978-3-15-0181256-6.

Scharlau, Ingrid (2007). *Jean Piaget zur Einführung*. 1. Auflage. Hamburg: Junius Verlag. 171 Seiten. ISBN: 978-3-88506-646-0.

Schnotz, Wolfgang (2006). *Pädagogische Psychologie. Workbook*. 1. Auflage. Weinheim: Beltz. 204 Seiten. ISBN: 978-3621275347.

Schumacher, Stefan (2009*a*). „Admins Albtraum. Die psychologischen Grundlagen des Social Engineering, Teil I". In: *Informationsdienst IT-Grundschutz* 7 (Juli 2009), Seiten 11 – 13. ISSN: 1862-4375. URL: `http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_7-2009_11_13.pdf` (besucht am 22. 07. 2009).

– (2009*b*). „Admins Albtraum. Die psychologischen Grundlagen des Social Engineering, Teil II". In: *Informationsdienst IT-Grundschutz* 8 (August 2009), Seiten 8 – 9. ISSN: 1862-4375. URL: `http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_8-2009_8_9.pdf` (besucht am 24. 08. 2009).

– (2009*c*). „Admins Albtraum. Die psychologischen Grundlagen des Social Engineering, Teil III". In: *Informationsdienst IT-Grundschutz* 10/11 (Oktober 2009), Seiten 21 – 22. ISSN: 1862-4375.

– (2009*d*). „Psychologische Grundlagen des Social-Engineering". In: *Proceedings des GUUG Frühjahrsfachgespräches 2009*. Band 2009. 10. – 13. März 2009, Hochschule Karlsruhe. Köln: GUUG, Seiten 77–98. ISBN: 978-3-86541-322-2.

Secrétariat général de la défense nationale, Herausgeber (2004). „Die Verteidigung in der Tiefe angewandt auf IT-Systeme (Memento)". In: URL: `http://www.ssi.gouv.fr/de/vertrauen/documents/methods/mementodep-V1.1_de.pdf`.

Weizenbaum, Joseph (2003). *Die Macht der Computer und die Ohnmacht der Vernunft*. 17. Auflage. Frankfurt: Suhrkamp. 368 Seiten. ISBN: 978-3518278741.