Berücksichtigung des Menschen in der Informationssicherheit mit dem Persönlichkeitsmodell von Julius Kuhl

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen
der Wirtschaftswissenschaftlichen Fakultät
der Leibniz Universität Hannover

vorgelegt von:
Marco Dismer
[redacted]

Erstprüfer: Prof. Dr. Michael H. Breitner
Hannover, den 9. Januar 2008

Inhaltsverzeichnis

1. Einleitung

1.1 Ausgangspunkt, Problemstellung und Zielsetzung

„Menschen spielen eine zentrale Rolle bei der Nutzung von IT-Systemen, die zur Erledigung nahezu aller Aufgaben genutzt werden. Daher ist es von äußerster Wichtigkeit, den »Faktor Mensch« in einer unternehmensweiten IT-Sicherheit entsprechend seiner Bedeutung in den IT-Sicherheitsprozeß mit einzubeziehen.“[1] Dieses Zitat weist auf zwei elementare Fakten der IT-Sicherheit hin. Zum einen ist dies die zunehmende Abhängigkeit der Unternehmen von ihren IT-Systemen, da ohne diese ein Arbeiten häufig kaum möglich ist. Dies verdeutlicht den Schutzbedarf und die Notwendigkeit einer möglichst einwandfreien Funktionsweise der IT-Systeme. Zum anderen wird der Faktor Mensch betont, der in der Praxis oft durch den Fokus auf technische Maßnahmen vernachlässigt wird.

Tatsächlich sind technische Maßnahmen zum Schutz der IT-Systeme weit verbreitet. So setzen fast 100% der Unternehmen Antiviren-Software ein und auch der Einsatz von Firewalls ist beinahe flächendeckend zu beobachten.[2] Weitere gängige technische Maßnahmen wie z.B. Passwortschutz und Verschlüsselung sollten den für die Informationssicherheit zuständigen Personen bekannt sein.[3] Auf der organisatorischen Ebene der Informationssicherheit helfen diverse Standards bei der erfolgreichen Umsetzung von Sicherheitsrichtlinien oder Sicherheitspolitiken.[4] Mit der Anwendung dieser bekannten Richtlinien und Maßnahmen lässt sich unter Berücksichtigung der Gesetze zum Datenschutz ein hohes Sicherheitsniveau erreichen.[5]

Neben diesen bekannten Sicherheitsmaßnahmen und den korrespondierenden Bedrohungen wird der Faktor Mensch häufig missachtet. Dies erstaunt umso mehr, da bei Sicherheitsvorfällen „in den meisten Fällen Irrtümer und Nachlässigkeiten bei den eigenen Mitarbeitern in der Organisation ausschlaggebend sind“[6]. Diese Aussage wird von verschiedenen Studien und Befragungen gestützt und in Abbildung 1 verdeutlicht.[7]

---

[1] Pohlmann, N. / Blumberg, H. [2004], S. 123.
[2] Vgl. dti [2006], S. 16 und S. 19.
[3] Vgl. Aebi, D. [2004], S. 60.
[4] Vgl. Witt, B. [2006], S. 42, Vgl. BSI (Hrsg.) [2005a], Vgl. BSI (Hrsg.) [2006a], Vgl. BSI (Hrsg.) [2006b].
[5] Vgl. Kersten, H. / Klett, G. [2005], S. 5, Vgl. Aebi, D. [2004], S. 15.
[6] Gora, W. / Krampert, T. (Hrsg.) [2003], S. 37.
[7] Vgl. kes [2006], S. 3, Vgl. dti [2006], S. 22.

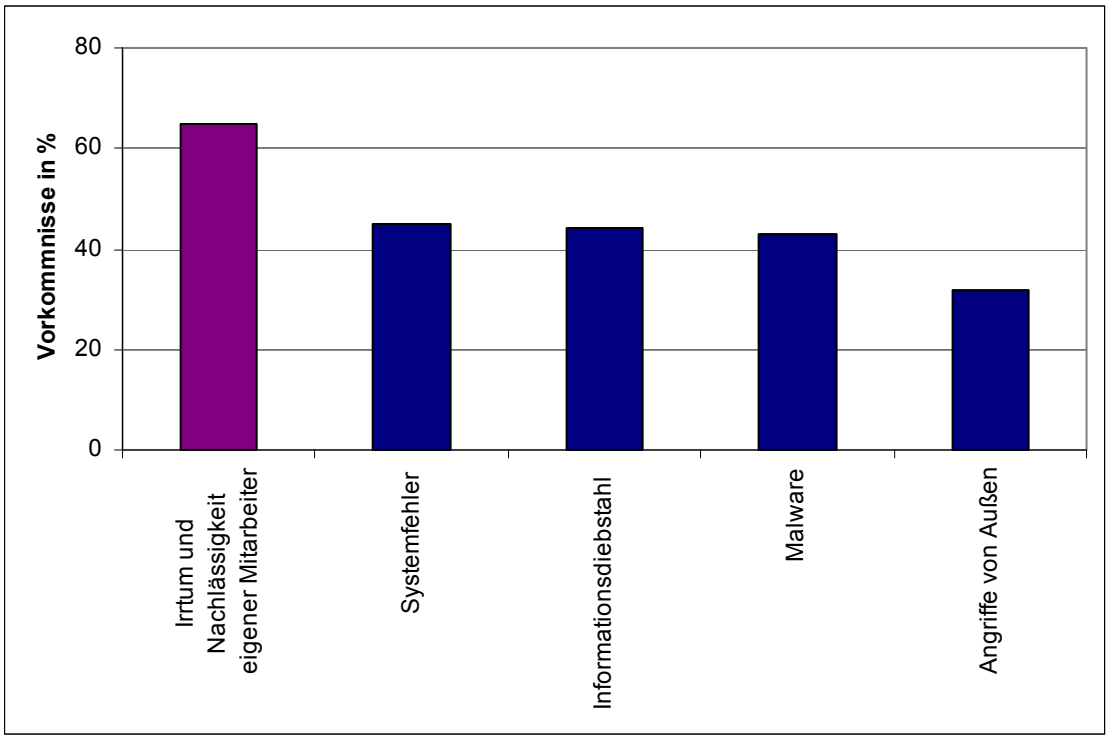

Abbildung 1: Ursachen der eingetretenen Gefährdungssituationen – dti Top 5 2006
Quelle: eigene Darstellung, Daten vgl. dti [2006], S. 22.

Besteht die Absicht, die Informationssicherheit zu verbessern, erscheint es sinnvoll, dieses grundlegende Problem anzugehen. Dabei stellt sich zwangsläufig die Frage, wie die Sensibilität der Mitarbeiter für das Thema IT-Sicherheit erhöht werden kann. Um langfristig die Informationssicherheit zu verbessern, muss zunächst verstanden werden, auf welchen Wegen der Mensch erreichbar ist. Das bedeutet, dass die Psychologie des Menschen berücksichtigt werden sollte.

Mit Hilfe von Persönlichkeitstheorien, im Rahmen dieser Arbeit speziell mit dem Fünf Faktoren Modell und der Persönlichkeits-System-Interaktionen Theorie, sollen die Eigenschaften einer Person und die Ursachen für das typische Verhalten analysiert werden. Dabei steht das Ziel im Mittelpunkt, Möglichkeiten zu finden, die die Sensibilität der Mitarbeiter für das Thema Informationssicherheit steigern. Im Idealfall entwickelt diese Arbeit ein allgemein anwendbares Konzept, mit dem Unternehmen die Sensibilität der einzelnen Mitarbeiter und letztendlich auch die Informationssicherheit gezielt erhöhen können.

1.2 Aufbau und Struktur der Arbeit

Die Arbeit nähert sich der vorgestellten Thematik zunächst durch eine grundlegende Betrachtung der Informationssicherheit an. Dies geschieht im zweiten Kapitel, in dem zunächst einige Definitionen gegeben werden. Dabei wird auch der Begriff Informationssicherheit umfassend erläutert. Danach werden die verschiedenen Aspekte der Informationssicherheit betrachtet und in technische, rechtliche, ökonomische und organisatorische Aspekte unterteilt. Abschließend werden die Gefährdungen für die Informationssicherheit vorgestellt, wobei der Faktor Mensch und seine besondere Rolle betont werden.

Von der Betrachtung des Menschen als Risiko für die Informationssicherheit findet im dritten Abschnitt der Übergang zur psychologischen Betrachtungsweise statt. Auch hier kommt es zunächst zu einigen allgemeinen Erläuterungen, bevor das Fünf Faktoren Modell der Persönlichkeit vorgestellt wird. Im Anschluss folgt die Darstellung der umfangreichen PSI-Theorie. Auf Grund des Umfangs wird zunächst ein grober Überblick gegeben, bevor die einzelnen Komponenten detailliert dargestellt werden. Der dritte Abschnitt endet mit einem ganzheitlichen Überblick über die zuvor dargestellte PSI-Theorie.

Im vierten Abschnitt wird zunächst auf die praktische Anwendbarkeit des Fünf Faktoren Modells eingegangen. Darauf folgt die Anwendung der PSI-Theorie auf verschiedene exemplarische Persönlichkeitsstile, die zuvor vorgestellt werden. Kern des vierten Kapitels ist die kombinierte Anwendung des Fünf Faktoren Modells und der PSI-Theorie in einem Konzept zur Verbesserung der Informationssicherheit.

Abschließend gibt das fünfte und letzte Kapitel einen Gesamtüberblick über die Kerninhalte der Diplomarbeit und bietet einen kurzen Ausblick auf zu erwartende Entwicklungen. Der gesamte Aufbau der Diplomarbeit ist in Abbildung 2 dargestellt.

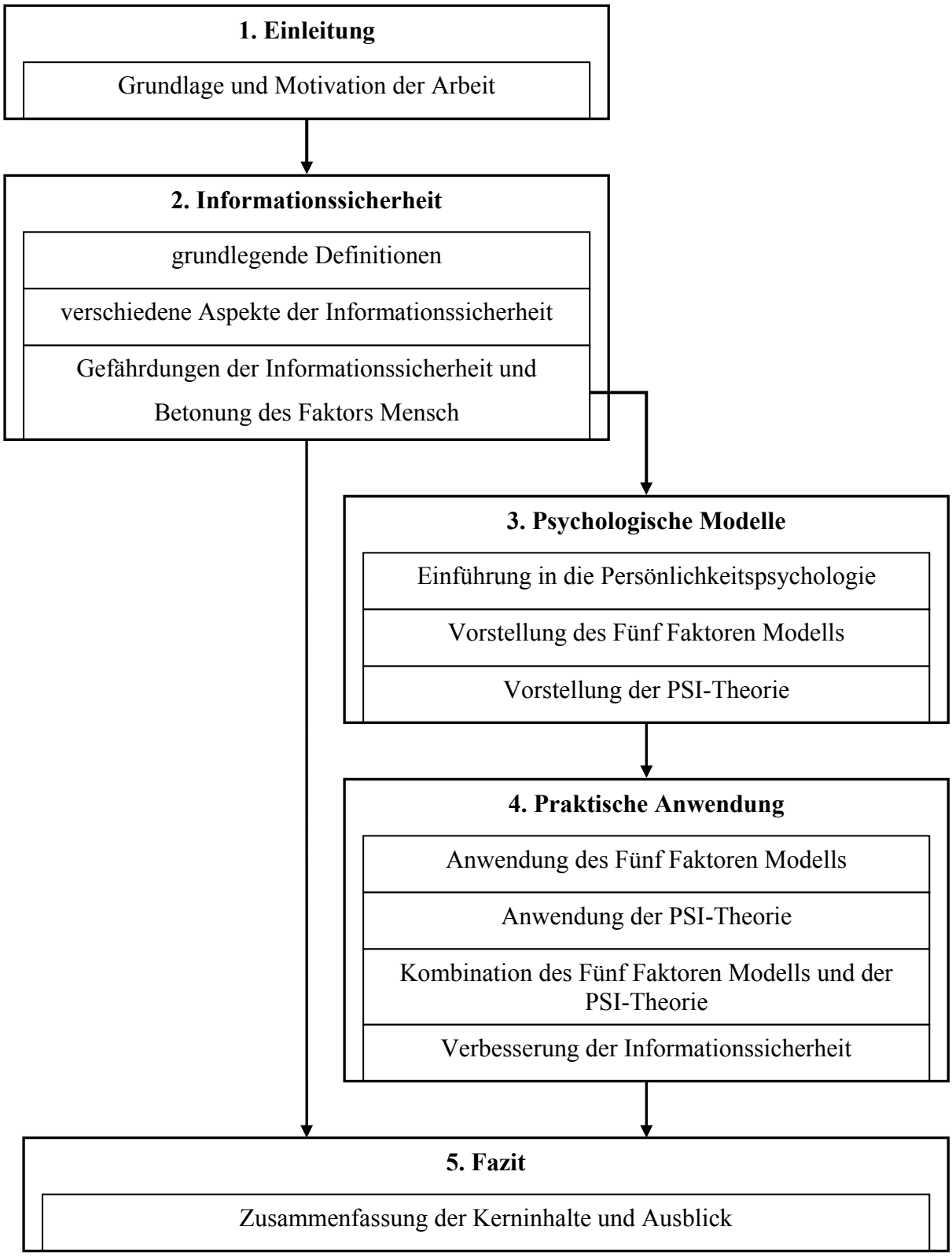

Abbildung 2: Schematische Darstellung des Aufbaus der Diplomarbeit
Quelle: eigene Darstellung

erfolgreicher als bei Standardschulungen oder der Vermittlung durch Broschüren. Da das gezeigte Vorgehen für eine einzelne IT-Abteilung in einem Unternehmen sehr umfangreich ist, ist es denkbar, standardisierte Zuordnungen zwischen einem Fragebogenergebnis und der entsprechenden idealen Schulungsgruppe zu entwickeln. Dies kann bspw. in Form einer Zuordnungstabelle geschehen, mit deren Hilfe die Ergebnisse des NEO-Pi-R-Fragebogens direkt einem Persönlichkeitsstil und somit indirekt auch einer Schulung zugewiesen werden. Der komplizierte Prozess, bei dem jeder einzelne Mitarbeiter einem Persönlichkeitsstil zugeordnet würde so verkürzt.

Die Entwicklung der angepassten Schulungsinhalte wird das Aufgabengebiet und die Kompetenzen einer üblichen IT-Abteilung überschreiten, da die Kenntnisse im Bereich der Persönlichkeitspsychologie minimal oder nicht vorhanden sein dürften. Hier empfiehlt sich die Einbeziehung von Experten, die die angepassten Inhalte entwickeln und aktualisieren. Der gesamte Schulungsprozess von der Durchführung des NEO-Pi-R-Fragebogens bis hin zur eigentlichen Schulung könnte an einen externen Dienstleister abgegeben werden. Dadurch hätten auch kleinere Unternehmen die Möglichkeit, ihre Mitarbeiter an einer solchen spezialisierten Schulungsmaßnahme teilnehmen zu lassen.

5. Fazit

Um Verbesserungsmöglichkeiten der Informationssicherheit zu entwickeln, wurde im zweiten Abschnitt dieser Arbeit zunächst das übliche Verständnis der Informationssicherheit dargestellt. Dabei wurde die Kategorisierung in die „Sicht der Verlässlichkeit“ und die „Sicht der Beherrschbarkeit“ vorgenommen und die dazugehörigen Dimensionen vorgestellt. Danach wurden die technischen, rechtlichen, ökonomischen und organisatorischen Aspekte erläutert. Des Weiteren wurden die verschiedenen Bedrohungen für die Informationssicherheit und besonders der Mensch als wesentlicher Bestandteil und gleichzeitig auch als Schwachpunkt der Informationssicherheit identifiziert.

Im anschließenden dritten Abschnitt wurde zunächst das Fünf Faktoren Modell vorgestellt. Dieses Modell wurde im weiteren Verlauf der Arbeit als Grundlage zur Bestimmung von Persönlichkeitsstilen genutzt. Die Bestimmung der vorliegenden Persönlichkeitsstile bei den Mitarbeitern erfolgte durch die Anwendung des NEO-Pi-R-Fragebogens, der auf dem Fünf Faktoren Modell basiert. Weiterhin wurde die deutlich komplexere PSI-Theorie vorgestellt, mit der sich die Gründe für die Handlungen und die Persönlichkeit von Menschen erklären lassen.

Mit dieser Theorie ist es möglich, den Mensch in der Informationssicherheit nicht nur zu berücksichtigen, sondern durch die Unterteilung in die vorgestellten Persönlichkeitsstile gezielt auf die individuellen Stärken und Schwächen der einzelnen Personen einzugehen. Dabei wird deutlich, dass sich die Persönlichkeitsstile der einzelnen Menschen durch verschiedene Ausprägungen interner Makrosysteme und Affekte auszeichnen. Auf Grundlage dieser Erkenntnisse ist es möglich, jeden Menschen in Abhängigkeit der Ausprägungen der Systeme und Affekte auf eine bestmögliche Art und Weise zu erreichen, indem die aktivierten Systeme genutzt werden. In einem gewissen Rahmen ist es auch möglich, durch bestimmte Affekte von außen die Systemkonfiguration zu beeinflussen.

Die praktische Anwendung, die Parallelen und die kombinierte Anwendung des Fünf Faktoren Modells und der PSI-Theorie wurden im vierten Abschnitt aufgezeigt. Die Parallelen sind bei der Zuordnung der Mitarbeiter in eine geeignete Schulungsgruppe wichtig, sollten aber weiter untersucht werden, um eine präzise, wissenschaftlich fundierte Zuordnung zu ermöglichen. Gleiches gilt auch für die vorgeschlagenen Gestaltungen der Schulungen. Auch hier ist sicherlich eine weitere Untersuchung und Entwicklung geeigneter Maßnahmen sowie eine spezifischere Abstimmung auf die Persönlichkeitsstile möglich.

Es ist fraglich, ob ein Unternehmen die Theorien der Persönlichkeit selbst studiert, um die Mitarbeiter für die Informationssicherheit zu sensibilisieren. Dem im vierten Abschnitt vorgestellten Vorgehen zur Sensibilisierung der Informationssicherheit liegt die umfangreiche PSI-Theorie zu Grunde. Ein grundlegendes Verständnis des Zusammenwirkens der dazugehörigen Makrosysteme und der Bedeutung der Affekte ist für die weitere Anwendung des Konzepts notwendig. Auch die Zuordnung der Ergebnisse des Fünf Faktoren Modells zu den Persönlichkeitsstilen führt zu einem komplexen Vorgehen. In der Praxis fehlen unter Umständen Zeit und Geld, so dass auf eine allgemeine Schulung zurückgegriffen wird, die die Persönlichkeitsunterschiede nicht berücksichtigt.

Eine Möglichkeit zur Vereinfachung der Anwendung ist die Entwicklung eines Fragebogens, der direkt auf die von *Kuhl* genannten Persönlichkeitsstile und die PSI-Theorie ausgerichtet ist, so dass der NEO-Pi-R-Fragebogen und somit auch die aufwändige Zuordnung der Ergebnisse entfällt. In einem solchen Prozess ist die Berücksichtigung des Fünf Faktoren Modells nicht nötig, da die Ergebnisse eines solchen neuen Fragebogens eine direkte Zuordnung der Persönlichkeitsstile ermöglichen.

Denkbar ist auch, dass die Schulungen durch externe Dienstleister durchgeführt werden. Diese könnten sich besser mit einem umfassenden Konzept und der umfangreichen PSI-Theorie auseinandersetzen, als dies die IT-Abteilung innerhalb eines Unternehmens vermag. Auch die Entwicklung der Schulungsinhalte durch einen externen Dienstleister ist sinnvoller, da er diese für die Mitarbeiter verschiedener Unternehmen einsetzen kann. Hier stellt sich allerdings die Frage, ob zunächst ein Angebot oder eine Nachfrage vorhanden sein muss, damit solche Schulungen von Dienstleistern entwickelt und angeboten werden.

Dass Handlungsbedarf besteht, wurde besonders durch die Umfragen gezeigt. Die Mitarbeiter stellen laut verschiedener Umfragen das jeweils größte Gefahrenpotential für die Informationssicherheit dar. Diese Ergebnisse verdeutlichen, dass das Problem bekannt ist. Als Konsequenz ist zu erwarten, dass die Sensibilisierung der Mitarbeiter weiter in den Mittelpunkt rückt. Problematisch ist die gleichzeitig vorliegende finanzielle Knappheit[371], die teuere Neuentwicklungen, in diesem Fall die Entwicklung der Schulungsinhalte, besonders schwierig macht. Der hohe Aufwand, den die Berücksichtigung einer Persönlichkeitstheorie mit sich bringt, spricht eher gegen einen Einsatz eines solchen Konzepts in der Praxis. Diesen beiden Kritikpunkten kann allerdings mit der genannten Nutzung externer Dienstleister begegnet werden. Die Berücksichtigung des Menschen und seiner Persönlichkeitsausprägungen ist definitiv sinnvoll. Denn wer es schafft, die Mitarbeiter nachhaltig zu sensibilisieren, wird ein höheres Sicherheitsniveau und eine Abnahme der Sicherheitsvorfälle erreichen. Dies führt in der Folge zu einer Kostenersparnis. Die gezielte Sensibilisierung der Mitarbeiter stellt eine Investition in die Zukunft dar, mit der die Informationssicherheit durch die Berücksichtigung der Persönlichkeitsmerkmale nachhaltig gesteigert werden kann.

[371] Siehe Abbildung 14, S.49.