Auswirkungen ausgewählter Persönlichkeitsmerkmale auf die Informationssicherheit: Technische und organisatorische Aspekte

Diplomarbeit

zur Erlangung des Grades einer Diplom-Ökonomin der

Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Dogan Vorname: Dilek

[redacted]

Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, den 26.11.2010

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation

"Das Übel kommt nicht von der Technik, sondern von denen, die sie missbrauchen - mutwillig oder auch nur fahrlässig." - Jacques Yves Cousteau -

Wir haben uns in den letzten Jahrzehnten von der industriellen zur dienstleistungsorientierten Gesellschaft gewandelt. Dies bedeutet, dass wir in immer stärkerem Masse von Informationen abhängig sind. Hinzu kommt, dass sich unsere Wirtschaft und damit weite Teile unseres Lebens, in sehr kurzer Zeit globalisiert haben. Globalisierung bedeutet, dass wir uns in einer interkulturellen, zeitlich und räumlich zusammenwachsenden Umgebung befinden. In dieser globalisierten Welt sind die komplexen Aufgaben in Unternehmen ohne eine funktionierende IT (Informationstechnik) nicht mehr lösbar. Informationen und Prozesse müssen rund um die Uhr an jedem Ort der Welt zuverlässig verfügbar sein. Es zeigt sich, dass die Unternehmen, Länder und Eco-Systeme am erfolgreichsten sind, die sich am stärksten vernetzt haben. Diese Vernetzung findet dabei nicht nur in geschlossenen Systemen also in Unternehmen oder zwischen zusammenarbeitenden Unternehmen statt. Vielmehr vernetzen sich Unternehmen immer mehr direkt mit ihren Kunden. Ganze Fertigungs- und Vertriebsketten sind heute auf die Online Kommunikation ausgelegt. Diese immense Abhängigkeit stellt zwangsläufig immer höhere Anforderungen an den IT-Betrieb. Die Kommunikation muss dabei nicht nur schnell, sicher und zuverlässig sein, sondern auch im besonderen Masse vertrauenswürdig.

In technischer Hinsicht wurden in den letzten Jahren permanent Verbesserungen an der Verfügbarkeit, der Geschwindigkeit und an der Datenintegrität erreicht. Systeme sind heute nicht nur redundant ausgelegt sondern in der Wolke des Internets mehrfach und sehr skalierbar erreichbar. Die Bandbreiten im Internet stoßen in Bereiche vor, die alle heute erdenklichen Anwendungen abbilden können und die Verschlüsselung der Kommunikation ist so stark, dass defacto kein Einbruch möglich ist. In der weiteren Entwicklung wurden Prozesse und Standards etabliert, die den gewachsenen Anforderungen der IT-Sicherheit Rechnung tragen. Sicherlich ist eine 100 prozentige Sicherheit eine Illusion. Die Technologie und Sicherheitsstandards haben uns aber ein ganzes Stück in dem Streben danach voran gebracht. Trotzdem muss immer ein Kompromiss zwischen der Effizienz von Sicherheitsmaßnahmen, ihrer Nutzbarkeit und ihrer Wirtschaftlichkeit gefunden werden.

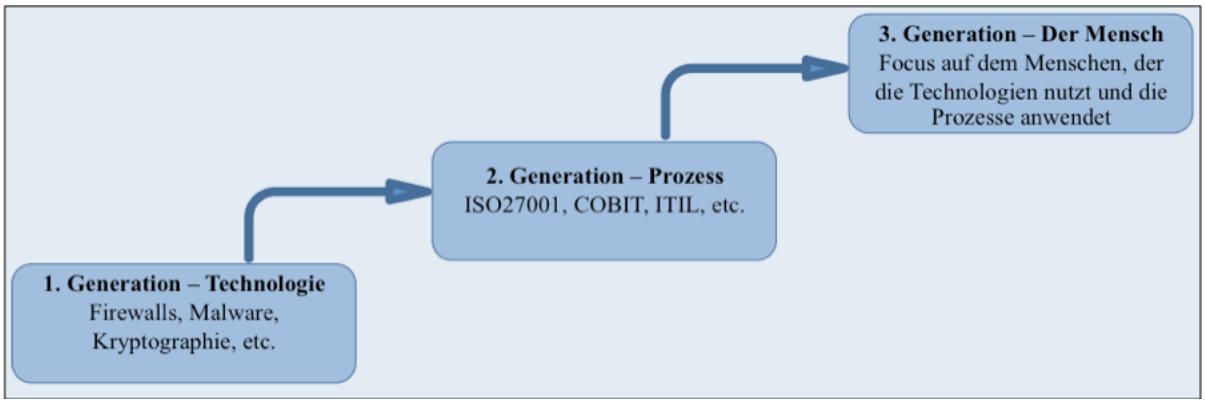

Abbildung 1: Evolution der Informationssicherheit
Quelle: Eigene Darstellung an Vgl. Dontamsetti/Narayanan (2009), S. 28.

Aber welche Rolle spielt dabei der Faktor „der Mensch“? In unserem Bewusstsein ist der Faktor Mensch als Sicherheitsrisiko eher unterrepräsentiert und wenig erforscht. Die Firma Ontrack hat 2005 in einer Studie[1] zu diesem Thema ihre Kunden befragt. Dabei kam heraus, dass hingegen der verbreiteten Meinung nicht 11% sondern 26% der Datenverluste auf Anwenderfehler zurückzuführen sind. Bei der gleichen Studie im Jahr 2010 glaubten 40% der Anwender an menschliche Fehler als Ursache für Datenverluste. Allerdings lag der tatsächliche Anteil mit 27% ähnlich hoch wie 2005. Diese Diskrepanz zeigt, wie wenig wir uns immer noch mit dem Thema beschäftigen. Sie zeigt aber auch, dass der Faktor Mensch einen sehr hohen Anteil an den Auswirkungen einer IT-Sicherheitsstrategie hat. Daher sollten Unternehmen ihre IT-Sicherheitsplanungen nicht nur an dem technologisch Machbaren sondern im starken Masse an den sie integrierenden Menschen ausrichten. Das bedeutet, dass bei der Erarbeitung von Sicherheitsstrategien im IT-Bereich die Psychologie des Menschen berücksichtigt werden muss, um die Ursachen für deren Handeln und Denken miteinzubeziehen. Da unterschiedliche Charaktere sicherlich in unterschiedlichem Masse gefährdend sind, stellt sich dann die Frage ob es Zusammenhänge zwischen Persönlichkeitsmerkmalen und deren Auswirkung auf die IT-Sicherheit gibt.

In der nachfolgenden Arbeit soll versucht werden, diese Frage an Hand von einigen ausgewählten Merkmalen zu beantworten. Das Ziel soll sein, Handlungsempfehlungen für die Implementierung von Technologien und die damit verbundenen organisatorischen Maßnahmen bei der Umsetzung von Sicherheitsstandards zu entwickeln. Dabei soll im Mittelpunkt stehen, dass die größtmögliche Sicherheit gewährleistet werden kann, ohne dabei die Kerngeschäftsbereiche eines Unternehmens zu behindern. Als Grundlage für die Ausarbeitung der theoreti-

[1] Vgl. Kroll Ontrack (2010).

schen Annahmen wird auf bestehendes Datenmaterial zurückgegriffen und zur Unterstützung der praktischen Validierung wird eine Expertenbefragung von IT-Entscheidern und Beratern durchgeführt. Auf Grund der Komplexität der menschlichen Psyche und den individuellen Handlungen ist es natürlich illusorisch, eindeutige Richtlinien zu erarbeiten. Vielmehr ist das Ziel dieser Arbeit, Zusammenhänge darzustellen und IT-Entscheider dabei zu unterstützen, die Mitarbeiter im Unternehmen für die Informationssicherheit zu sensibilisieren und die Akzeptanz für die entsprechenden technischen und organisatorischen Lösungen zu erhöhen.

Der Mensch ist fehlbar und wird es immer bleiben. Der Nachweis für diese menschliche Imperfektion ist in nahezu allen religiösen und mythischen Texten zu finden. Egal wie technisch entwickelt und komplex eine Lösung ist so steht am Ende immer der Nutzer. Daher müssen wir immer bedenken dass das System für den Einzelnen nutzbar bleibt und für das Unternehmen einen Nutzen bringt.

1.2 Forschungsfrage und Zielsetzung

Im Rahmen dieser Arbeit soll nun der Frage nachgegangen werden, ob sich bestimmte Persönlichkeitsmerkmale in nachvollziehbarer Weise auf die Informationssicherheit auswirken und welche technischen und organisatorischen Aspekte entsprechend beachtet werden sollten.

Wie bereits oben erwähnt steht für viele Unternehmen die Information in einem besonderen Verhältnis zum Erfolg. Hierzu ist es von Bedeutung die Ursachen und Gründe für das menschliche Verhalten und Denken zu finden um durch die Berücksichtigung dieser die Informationssicherheit erhöhen zu können. Es soll herausgearbeitet werden, welche Wichtigkeit die Persönlichkeit und deren spezifische Merkmale für die Informationssicherheit hat, um so den Menschen im Umgang mit der IT besser kennenzulernen und möglichem Fehlverhalten präventiv entgegenzuwirken. Die Relevanz des Menschen und sein Verhalten, sollte bei allen technischen und organisatorischen Maßnahmen, die ein Unternehmen implementiert, miteinbezogen werden können.

Als Grundlage werden die Ergebnisse, die im Rahmen der Arbeit von Robert Pomes[2] am Institut für Wirtschaftsinformatik an der Leibniz Universität Hannover aufgezeigt wurden, verwendet. Die daraus ausgearbeiteten Hypothesen werden dann durch eine Expertenbefragung

[2] Robert Pomes: Doktorand der Leibniz Universität Hannover im Bereich Wirtschaftsinformatik.

überprüft. Dabei soll herausgefunden werden, ob die Ergebnisse in der Praxis nachvollziehbar sind und Zustimmung finden.

1.3 Aufbau und Methodik der Arbeit

Die vorliegende Arbeit gliedert sich in acht Kapitel. Im ersten Kapitel erfolgt eine Einführung in die Thematik und eine Darstellung der zugrunde liegenden Forschungsfrage mit dem beabsichtigten Ziel. Die notwendigen theoretischen Grundlagen der Informationssicherheit werden in Kapitel zwei abgefasst. Neben der umfassenden begrifflichen Erläuterung der Informationssicherheit werden die Gefahren, die Schwachstellen sowie die technischen und organisatorischen Perspektiven der Informationssicherheit näher betrachtet.

Die Kategorisierung des Menschen als Schwachstelle für die Informationssicherheit wird in Kapitel drei untersucht. Dabei stehen im Fokus dieses Kapitels die psychologische Betrachtung des Menschen und gängige Persönlichkeitstheorien. Nach einem historischen Abriss über die Entwicklung und Bedeutung der fünf Faktoren zur Erläuterung der Persönlichkeit werden Messinstrumente zur Bestimmung der Persönlichkeit vorgestellt.

Unter Verwendung dieser Grundlagen befasst sich das vierte Kapitel mit den Zusammenhängen von Persönlichkeitsmerkmalen in der Informationssicherheit. Anhand der verfügbaren Literatur werden Sachverhalte gesammelt und daraus Hypothesen abgeleitet. Als Basis für die Ausarbeitung werden die Ergebnisse aus der Studie von Robert Pomes verwendet. Dabei werden fünf interessante Korrelationen zwischen Persönlichkeitsmerkmalen und der technischen und organisatorischen Dimensionen der Informationssicherheit herausgearbeitet, die anschließend im Detail diskutiert werden.

Im Anschluss darauf erfolgt im fünften Kapitel eine empirische Untersuchung der ausgewählten Zusammenhänge. Nach einer Erläuterung zum Aufbau und der Methodik der empirischen Untersuchung werden die Ergebnisse ausgewertet. Mit der Validierung der Hypothesen werden mögliche Auswirkungen sowie Vor- und Nachteile der Persönlichkeitsmerkmale ausführlich dargestellt. Resultierend aus den Ergebnissen der empirischen Untersuchung werden im darauffolgenden sechsten Kapitel Handlungsempfehlungen für die Informationssicherheit unter Berücksichtigung der ausgewählten Persönlichkeitsmerkmale gegeben.

Abschließend werden im siebten und achten Kapitel nach einer kritischen Würdigung die Kerninhalte der Arbeit in einem Gesamtüberblick wiedergegeben. Der gesamte Ablauf der Arbeit wird in Abbildung 2 dargestellt.

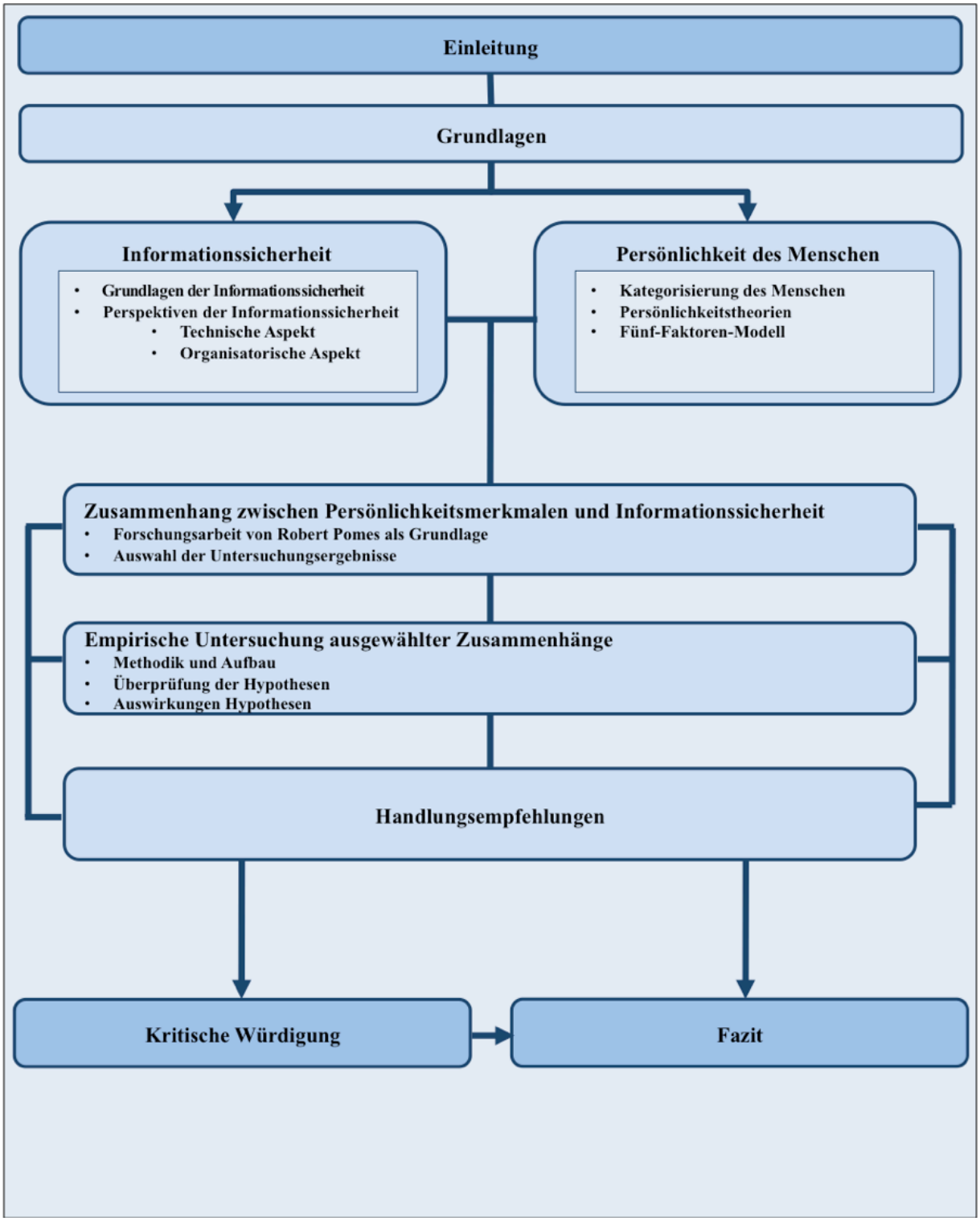

Abbildung 2 : Aufbau der Diplomarbeit
Quelle: Eigene Darstellung

8 Fazit

Ziel der vorliegenden Arbeit war es, die Auswirkung einiger ausgewählter Persönlichkeitsmerkmale auf die Informationssicherheit zu untersuchen. Dabei sollten sowohl die technischen als auch die organisatorischen Aspekte berücksichtigt werden. Es sollte auch überprüft werden, ob die Persönlichkeitsmerkmale einen Rückschluss auf das Verhalten der Menschen im Rahmen der Nutzung von Informationstechnologien zulassen.

Zunächst wurden die zur Verfügung stehenden theoretischen Grundlageninformationen der Informationssicherheit herausgearbeitet. Diese wurden in technischer und organisatorischer Hinsicht im Zusammenhang mit der Verlässlichkeit und Beherrschbarkeit von Informationstechnologien detailliert beschrieben. Im Anschluss wurde der Faktor Mensch als Schwachstelle und danach die Grundlagen der Theorien über die Persönlichkeitsmerkmale und die damit zusammenhängenden psychologischen Betrachtungen erörtert. Dabei wurde im Besonderen auf das Fünf-Faktoren-Modell mit den faktoranalytischen Messinstrumenten NEO FFI und dem etwas umfangreicheren NEO PI-R zur psychologischen Operationalisierung der Persönlichkeitsmerkmale eingegangen.

Basierend auf dieser Ausarbeitung wurden anhand der verfügbaren Literatur Sachverhalte zusammengetragen und 5 Hypothesen abgeleitet, die im weiteren Verlauf der Arbeit eingehend diskutiert wurden. Als Ausgangspunkt wurden dabei die Ergebnisse der Studie, die im Rahmen der Dissertation von Robert Pomes ermittelt wurden, verwendet.

Neben der Zusammenstellung der Hypothesen wurde im Hauptteil der Studie ein besonderer Schwerpunkt auf die empirische Untersuchung zur Validierung der ausgewählten Zusammenhänge gelegt. Diese Datenerhebung wurde im Feld mittels Experteninterviews durchgeführt um eine größtmögliche Praxisnähe zu erreichen. Die Auswertung dieser Daten ergab, dass das grundlegende Thema dieser Arbeit auf Interesse stößt und dass der Einfluss der Persönlichkeit auf die Informationssicherheit anerkannt wird. Allerdings wird auch festgestellt, dass die Materie sehr theoretisch ist und derzeit in der Praxis kaum Anwendung findet. Generell ist zu sagen, dass nur wenige Erfahrungen auf diesem Gebiet bei den Probanden vorgefunden werden konnten. Am häufigsten wurden die herausfordenden Persönlichkeitsmerkmale wie hoher Neurotizismus und gering ausgeprägte Gewissenhaftigkeit als Risiko für die Informationssicherheit angesehen. Es konnten aber auch bei diesen Zusammenhängen einige positive Hand-

lungsempfehlungen herausgearbeitet werden. Anhand der Expertenmeinungen konnten sehr breit aufgestellte Vor- und Nachteile der einzelnen Hypothesen und den beschriebenen Auswirkungen auf die IT-Sicherheit aufgelistet werden. Interessant ist dabei, dass das Verhältnis zwischen positiven und negativen Auswirkungen in der Regel ausgewogen erscheint. Jede der diskutierten Hypothesen kann in der Praxis sowohl mit Vor- als auch mit Nachteilen assoziiert werden. Diese diversivizierten Aussagen können daher in umfangreichen Handlungsempfehlungen für die Zusammenarbeit von Entscheidern und Mitarbeitern in IT-Abteilungen zusammengefasst werden.

Im Wesentlichen kann gesagt werden, dass Personen mit sehr gering ausgeprägter Gewissenhaftigkeit oder mit sehr hohem Neurotizismus von vielen der befragten Experten als eher ungeeignet angesehen werden, verantwortliche Aufgaben im Rahmen der IT-Sicherheit zu übernehmen. Indes konnten aber auch für diese Personen Stärken und Vorteile herausgearbeitet werden. Allerdings wird vom überwiegenden Teil der Experten erwartet, dass verantwortliche Personen eher mit einer hohen Gewissenhaftigkeit charakterisiert werden können. Diese werden als motivierender gegenüber anderen und selbst motivierter und damit korrekter angesehen. Generell wurde von den Befragten auch angemerkt, dass die arbeitsrechtlichen Rahmenbedingungen unter Umständen es nicht zulassen, Strukturen und spezielle Maßnahmen die auf einzelne Personen ausgerichtet sind, in einem Unternehmen zu implementieren.

Abschließend kann behauptet werden, dass es Persönlichkeitsmerkmale von Mitarbeitern in der IT gibt, die bei signifikanter Ausprägung entscheidende Auswirkungen auf die Informationssicherheit haben. Dies gilt sowohl für die technischen Aspekte wie Betrieb und Konzeption von IT-Systemen aber vor allem auch für die organisatorischen Aspekte wie Ergonomie und das Verhältnis zwischen Kosten und Nutzen. Es empfiehlt sich daher in Anbetracht des Stellenwertes einer funktionierenden und vertrauenswürdigen IT, die Persönlichkeiten der Betreiber aber auch der Nutzer von Informationssystemen in der Zukunft mehr zu berücksichtigen. Dies wird sowohl die Akzeptanz und damit die Sicherheit, aber auch die Produktivität beim Einsatz von Informationstechnologien erhöhen.