Psychologische Analyse der Schwachstelle Mensch in Informationssystemen

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B. Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

Vorgelegt von

Name: Barczak Vorname: Meike

[redacted] [redacted] [redacted] [redacted]

Prüfer: Prof. Dr. M. H. Breitner

Hannover, den 11.08.2016

INHALTSVERZEICHNIS

1. EINLEITUNG

Diese Arbeit widmet sich dem wohl bedeutendsten Sicherheitsfaktor von Informationssystemen (IS): Dem Menschen. Die Ursprungsquellen von Gefahren sind vielfältig – sie reichen von Unzufriedenheit bis hin zu Missmut oder einer subjektiv empfundenen Bedrohung durch die Einführung von IS. Schließlich ist das Ersetzen menschlicher Arbeitskraft durch Technik schon lange in die Realität gerückt. Aber auch viele andere Aspekte machen die Diskussion des Menschen als Risikofaktor für IS aufgrund seiner natürlichen Fehlbarkeit unumgänglich.

Diese Arbeit widmet sich der Frage nach dem Hintergrund dieser Gefahren. Es wird auf psychologische Theorien und Konzepte zurückgegriffen, die den Versuch des *Verstehens* untermauern sollen. Je besser die Mitarbeiter verstanden werden, beziehungsweise je weiter man ihr Verhalten auf Muster und Ursachen zurückführen kann, desto effektiver und effizienter können Reaktionen auf den falschen Umgang mit IS ausfallen. In dieser Arbeit versuche ich Fragen hinsichtlich des Einflusses verschiedener Faktoren auf das Informationssicherheitsverhalten von Menschen zu beantworten. Dieser Gedankengang kann in Abbildung 1 nachvollzogen werden.

Die Menschen stolpern nicht über Berge, sondern über Maulwurfshügel.
Konfuzius

IS sind groß und komplex, oft greift eine unüberschaubare Anzahl an Nutzern gleichzeitig auf sie zu – vor jedem Einzelnen kann ein „Maulswurfshügel“ aus dem Boden schießen. Das Ziel dieser psychologischen Analyse über Theorien und Konzepte ist das erfolgreiche Umgehen, Überspringen, Hindurchscharren, oder auch nur das Vermeiden eines Stolperns durch adäquate Maßnahmen mit gleichzeitiger Berücksichtigung von Moral und Ethik.

Ich erwarte, dass sich dabei Forschungslücken ergeben werden. Anschließend werde ich Verbindungen zwischen den Erklärungen ziehen und die Frage beantworten, inwiefern sich die Gefahren durch das menschliche Denken, Verhalten und Moral erklären lassen. Die möglichen resultierenden Maßnahmen werden nachfolgend auf ihre Umsetzbarkeit überprüft. Hieraus entsteht eine Forschungsfrage dieser Arbeit: Können Menschen auf Grundlage dieser Erklärungen, begründet auf psychologischen Theorien, unterstützt werden?

Im Anschluss dieser Einleitung findet sich eine MindMap, die den intellektuellen Prozess der Themenfindung illustriert. Ausgangsidee waren psychologische Konzepte allgemein, die sich gut auf Menschen im Umgang mit IS und den damit zusammenhängenden Sicherheitsaspekten übertragen lassen.

Warum aber ist der Mensch so wichtig? Er ist aus allen Abteilungen eines Unternehmens auch in Zukunft nicht wegzudenken – jedenfalls noch nicht. Solange es keine Roboter gibt, die andere Roboter reparieren und wiederum von einem dritten instandgehalten werden können, braucht es einen Menschen, der sich beispielsweise um die ordnungsgemäße Funktionsweise einer roboterbetriebenen Produktion kümmert. Außerdem verlangt es die aktuell geltende Ethik, ein optimales Maß an Kombination von Mensch und Maschinen zu finden und die Leistungserbringung unserer Spezies eben nicht vollständig durch Computer zu ersetzen.

Allgemein bekannt ist jedoch, dass der Mensch bei weitem nicht unfehlbar ist. Von ihm gehen klare Bedrohungen für IS, IT und deren Sicherheit aus, denen unbedingt entgegengewirkt werden muss. Das ist leichter gesagt als getan, denn Menschen sind mindestens so vielschichtig wie die von ihnen ausgehenden Bedrohungen: Zwei der am weitesten verbreiteten Gefahren ergibt sich durch externe Verursacher: Die „Infektionen der IT mit Malware (z. B. über das Internet oder über Wechseldatenträger) [oder] die soziale Manipulation von Mitarbeitern (Social Engineering)“. (Hertel, 2015) Die Einflussnahme darauf ist unternehmensintern besonders schwierig, denn an Kreativität und Organisation mangelt es den außenstehenden Angreifern nicht. Des Weiteren können durch Entwickler begangene Fehler – gewollt oder ungewollt – a priori verheerende Auswirkungen auf Geschäftsbeziehungen haben. (Hertel, 2015) Durch den Menschen entstehen außerdem noch ganz andere, einfachere Gefahren. Sie können beispielsweise dazu motiviert sein, ein System mutwillig zu zerstören oder zu sabotieren – etwa, wenn sie die Einführung eines neuen, komplizierten IS in seiner Notwendigkeit nicht begreifen vermögen. Auch fahrlässiges Verhalten kann zu Schäden führen, wenn dadurch Computerviren eingespeist werden oder eine allgemein falsche Handhabung realisiert wird. Es sind viele weitere Risiken wie Betrug, menschliches Versagen, Missbrauch, Diebstahl, oder Unwissenheit denkbar. (Breitner, 2015)

Einige dieser vielschichtigen Gefahrenquellen sollen in dieser Arbeit durch psychologische Konzepte ergründet werden, um eine nachstehende Analyse und die Entwicklung effektiver und effizienter Maßnahmengestaltung als Antwort auf die Erkenntnisse zu ermöglichen.

Um auf der Ebene des menschlichen Denkens nachdrücklichen Einfluss zu nehmen, muss man sich zunächst auf sie begeben und ergründen. Mitarbeiter und somit Menschen verlassen sich in gegebenen Situationen auf ihr Gefühl – das liegt in der Natur und ist unvermeidbar. Der Anspruch dieser Arbeit ist deshalb, dieses Gefühl in den kritischen Momenten zu sensibilisieren und zu schärfen. (Beaudry et. al, (2010)

Um diese Schwachstellenanalyse gut theoretisch zu fundieren, wird an erster Stelle eine Literaturanalyse durchgeführt, die vor allem helfen soll, Lücken in der bisherigen Forschung aufzudecken. Einen besonderen Fokus lege ich auf die Inbetrachtziehung der menschlichen Moral. Diese Thematik ist aktuell ein aufstrebendes Forschungsthema und soll aus diesem Grund ein besonderer Bestandteil der Analyse sein. Diese Grundlagen werden anschließend erweitert um allgemeine Ausführungen über die psychologischen Konzepte und Theorien, auf die alle Ausführungen zurückgehen werden. Selbige werden anschließend genutzt, um unter besonderer Berücksichtigung der menschlichen Moral erste Unterstützungsansätze für Systemnutzer zu entwickeln. Sie werden später zur Herleitung der Implikationen für die Praxis genutzt.

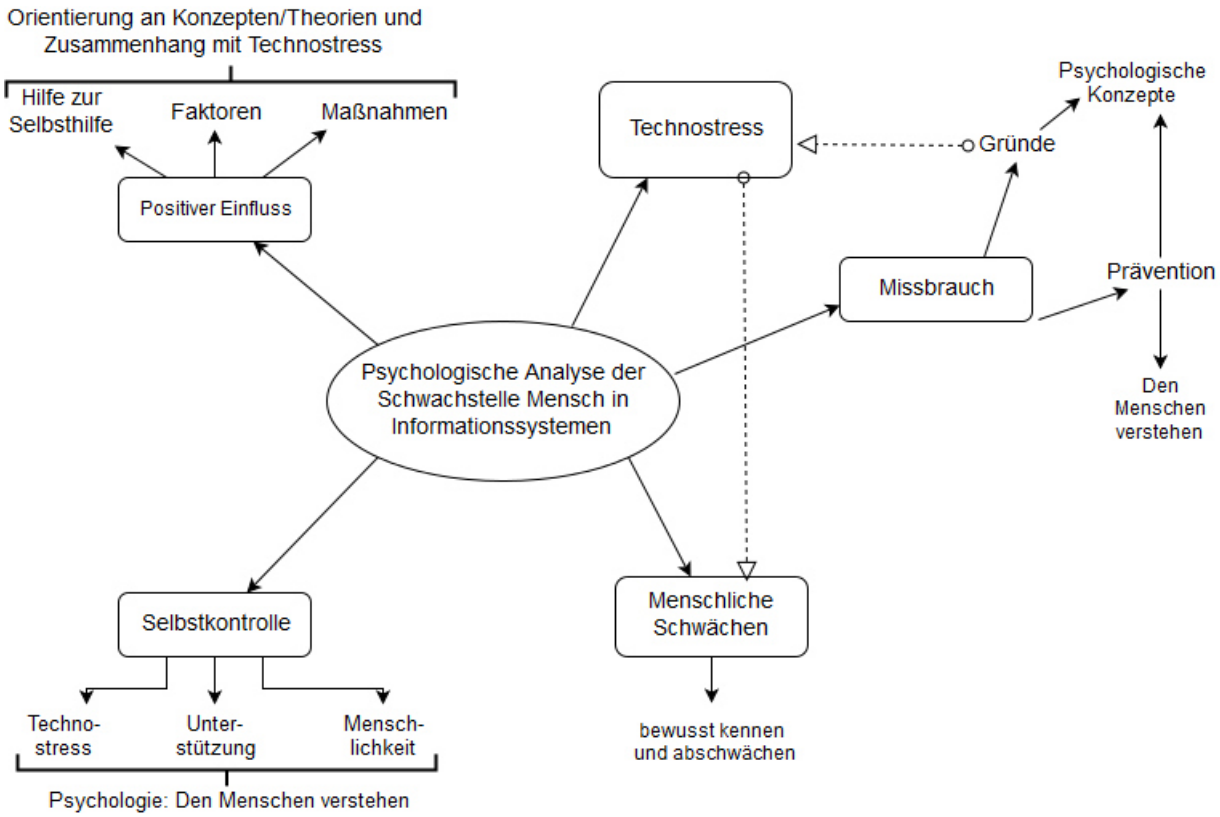

Abbildung 1: Gedankengang der Themenfindung
Quelle: Eigene Erhebung

8. FAZIT UND AUSBLICK

Im Rahmen dieser Arbeit konnte ich zeigen, dass eine genauere Betrachtung der Schwachstelle Mensch unter psychologischen Aspekten durchaus lohnend sein kann und auch für die Zukunft noch relevant ist. Außerdem ist klargeworden, welche bisher weitgehend unbeachtet gebliebene Funktion die Moral innehat. So konnte eine Forschungslücke aufgedeckt und viel Raum für die zukünftige Forschung geschaffen werden. Eine Schlüsselrolle spielt dabei das erfolgreiche Verbinden der Theorien, vor allem mit Technostress. So ist nun der Grundstein für eine innovative Kombination der Theorien gelegt, auf ihm aufbauend können auch Schlüsse für vergangene Studien gezogen werden. Darüber hinaus kann der generelle Einsatz der SAT durch die Erkenntnisse dieser Arbeit potenziell vorangetrieben werden und so zu ganzheitlicheren Ansätzen führen, die auch bspw. Gefühle, Moral und komplexere psychologische Zusammenhänge mit einbeziehen.

Die Kernbotschaft dieser Arbeit ist, dass Menschen egal in welcher Situation auch als solche behandelt werden sollten. Wie bereits gesagt, erfüllt ein gut durchdachtes Regelwerk keinen weiteren Zweck, wenn nicht ausreichend Anreize vorhanden sind, es nicht einzuhalten. Hier spielen viele unterbewusste und durchaus beabsichtigte Intentionen und Motivationen eine Rolle, die alle gleich stark bei den Überlegungen über Informationssicherheit berücksichtigt werden sollten. Eine kleine Auswahl habe ich in dieser Arbeit dargestellt – es gibt aber noch viele weitere psychologische Theorien und Konzepte, welche das Bild deutlich erweitern würden. In jedem Fall konnte ich darlegen, dass das Etablieren einer ansprechenden, unterstützenden Unternehmenskultur geboten sein sollte. Unabhängig von den einzelnen Theorien muss dieses Umfeld geschaffen werden, um den Mitarbeitern Handlungsräume zu geben, in denen sie sich frei bewegen können. Wenn machbar, sollten ferner Systeme integriert werden, die Fehler verzeihen und die Folgen menschlichen Versagens abschwächen.

Für die Zukunft stellt sich die Frage, welchen Stellenwert künstlichen Intelligenz einnehmen wird, welche längst kein abstraktes, irreales Konstrukt mehr ist. Sie rückt immer weiter in ein mögliches Bild der zukünftigen Realität. Wie diese Realität aufgrund der radikalen Einschnitte einer solchen Entwicklung sein und von der heutigen abweichen wird, kann man nur vermuten. Je nachdem, wie viel Einfluss der Mensch dann noch auf Geschehnisse hat (und ggf. haben will), ist die psychologische Grundlage der Menschheit kein bzw. nur noch ein geringfügig starker Risikofaktor hinsichtlich der Sicherheit von IS.

Abschließend sei gesagt, dass erneut die Wichtigkeit bereichsübergreifender Entscheidungen und Maßnahmen deutlich gemacht werden konnte. Ein vermeintlich weniger Ausschlag gebendes Kriterium bei der Auswahl von Mitarbeitern kann im Sinne der Informationssicherheit negative und positive Effekte auf den gesamten Unternehmenserfolg nach sich tragen. Aber auch, um allgemeine Unternehmensinteressen zielführend verfolgen zu können, sind diese Vorgänge von Bedeutung – es sei erneut die Unternehmenskultur von Einstellungsgesprächen bis hin zum Code of Conduct über den Umgang mit Gruppen und das gewählte Führungsverhalten genannt, die hierzu einen großen Beitrag leisten kann. Wie das möglich ist, wurde an diversen Stellen diskutiert. Zusammenfassend kann erneut die Studie von Beaudry et. al (2010) aufgeführt werden, die eindeutig die Relevanz von Gruppen bewiesen hat. Ihre Mitglieder können vor allem auch positiv unterstützend aufeinander wirken, wenn ein Einzelner Probleme mit der Nutzung von IS hat und entwickeln sich so zu einem Selbstläufer der Informationssicherheit.