Erfolgsmessung von IT-Sicherheitsschulungen: ein Vergleich von E-Learning und Präsenzveranstaltungen

Masterarbeit

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

vorgelegt von

Name: Lindemann Vorname: Jennifer Isabelle

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

Prüfer: Prof. Dr. M. H. Breitner

Ort, den: Güster, 10.09.2014

Inhaltsverzeichnis

Abbildungsverzeichnis……..IV

Tabellenverzeichnis……V

Abkürzungsverzeichnis……..VI

1. Einleitung……1

2. Theoretische Grundlagen……5

2.1. Experimente im Bereich der Informationssicherheit……5

2.2. Schulungsmethoden im Bereich der Informationssicherheit……..7

2.2.1. Präsenzschulung……8

2.2.2. E-Learning……10

2.3. Verhaltenstheorien im Bereich der Informationssicherheit……...11

2.3.1. Theorie der Schutzmotivation……12

2.3.2. Technologie Akzeptanz Modell……..13

3. Forschungsmodell und Hypothesenentwicklung……15

4. Methodik……...22

4.1 Design des Experiments und Teilnehmer……...22

4.2 Ziel des Experiments und Manipulation der Faktoren……...27

4.3. Versuchsdurchführung und Messung……..28

4.4 Zusammenfassung des Forschungsprozesses……..34

5. Analyse der Daten und Ergebnisse……..35

5.1. Demografisches Profil der Studie……35

5.2. Faktorenanalyse……..40

5.3. Strukturgleichungsmodellierung……43

5.4 Auswertung der Daten……46

5.5. Ergebnisse……54

6. Diskussion und Handlungsempfehlungen……...57

7. Limitationen……..63

8. Fazit……...65

9. Literaturverzeichnis……69

10. Anhang……...78

11. Ehrenwörtliche Erklärung……...98

1. Einleitung

Diese Arbeit behandelt das Themengebiet Informationssicherheit. Die grundsätzlichen Werte der Informationssicherheit sind Integrität, Verfügbarkeit und Vertraulichkeit (Bundesamt für Sicherheit in der Informationstechnik, 2008, S. 8). Informationssicherheit beinhaltet sowohl organisationale und rechtliche Aspekte als auch „best practices“ in Bezug auf Sicherheitstechnologien (Hagen et al., 2008, S. 377). Diese Arbeit wird sich auf organisationale Aspekte fokussieren, da dieser Bereich bisher, besonders der nicht-technische, noch nicht ausreichend erforscht wurde. Wissenschaftler fordern deshalb empirische Arbeiten zur Erforschung von erfolgsversprechenden Maßnahmen, die der Einhaltung von Sicherheitsvorschriften dienen (Siponen und Oinas-Kukkonen, 2007, S. 73). Die unternehmensbezogenen Sicherheitsvorschriften sind in grundsätzlichen Regeln festgehalten, die bestimmte Verhaltensweisen im Umgang mit Informationen festlegen (Ortalo, 1998, S. 68). Der Schutz der Informationen ist sehr wichtig für Unternehmen, da ein Verlust oder die Beschädigung dieser zu großen Schäden führen kann. Insbesondere deutsche Unternehmen müssen vermehrt auf den Schutz ihrer Informationen achten, da sich der Wettbewerbsdruck aufgrund der Globalisierung zunehmend erhöht. Dieses ist der Fall, da deutsche Unternehmen durch die Globalisierung auch mit Ländern konkurrieren, in denen der durchschnittlich zu zahlende Lohn wesentlich geringer ist. Aus diesem Grund ist es für Unternehmen der Industrieländer wichtig, ihre Unternehmensgeheimnisse zu bewahren und innovativ zu sein (Fussan, 2010, S. 264). Das Bundesamt für Informationssicherheit schätzt die Schäden, die im Zusammenhang mit der Informationssicherheit in Deutschland entstehen, auf 50 Milliarden Euro jährlich (Industrie- und Handelskammer, 2013, S. 1). Es sind allerdings nicht nur finanzielle Schäden möglich. Stellt man sich einmal vor, es würde ein Sicherheitsproblem in einem Chemieunternehmen geben. Hierdurch hätte ein Angreifer die Möglichkeit sowohl Menschen als auch die Umwelt in immens zu schädigen. Durch die große Reichweite eines Angriffs sind solche Unternehmen besonders attraktive Angriffsziele für Sabotage und Terrorismus und deshalb besonders schützenswert (Mahnke und Leitner, 2009, S. 203). In Abbildung 1 lassen sich die Risiken für deutsche Unternehmen erkennen. Es ist zu sehen, dass alle genannten Gefahren Bereiche der

Informationssicherheit betreffen. Durch diese Grafik wird deutlich, welchen Stellenwert die Sicherung der Unternehmensinformationen hat.

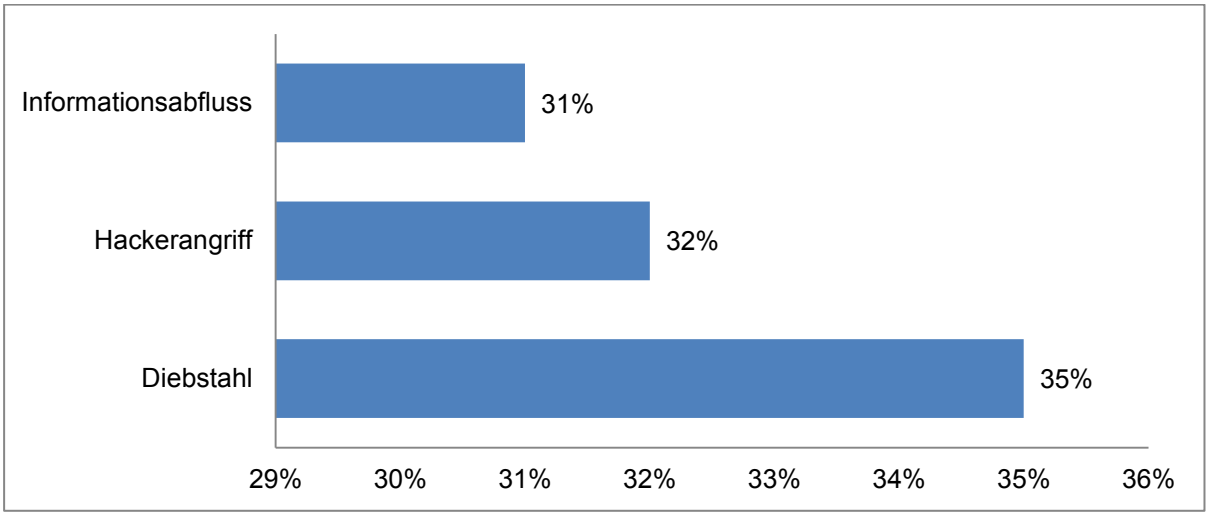

Abbildung 1: Risiken für deutsche Unternehmen (in Prozent)
Quelle: Gefahrenbarometer, 2010

Viele Forscher haben bereits bewiesen, dass der Mensch und damit der Mitarbeiter eines Unternehmens den größten Risikofaktor innerhalb der Informationssicherheit darstellt (z. B. Siponen, 2000, S. 197; Bulgurcu et al., 2010, S. 523). Daher ist es wichtig für Unternehmen wichtig zu erfahren, wie sie ihre Mitarbeiter beeinflussen können, sodass die Risiken für das Unternehmen minimiert werden. In der Literatur gibt es zahlreiche Vorschläge, durch welche es möglich sein soll, die Informationssicherheit im Unternehmen zu verbessern. Eine Umfrage der Unternehmensberatung Ernst & Young (2013) hat ergeben, dass 90% der befragten Manager eine zunehmende Gefahr der Informationssicherheit prognostizieren. Vor diesem Hintergrund ist es für die Unternehmen wichtig, die möglichen Alternativen zum Schutz der Unternehmensdaten zu kennen. Es gibt die Möglichkeit, technisch-administrative Maßnahmen einzuführen. Diese können beispielsweise Richtlinien oder Kontrollmechanismen sein. Laut der zuvor erwähnten Umfrage haben 88% der Unternehmen solche Maßnahmen bereits ergriffen (Ernst & Young, 2013). Allerdings muss hierbei erwähnt werden, dass diese Maßnahmen die Informationssicherheit nur zu einem gewissen Teil gewährleisten können. Um einen bestmöglichen Schutz zu erreichen, ist es deshalb wichtig, die technisch-administrativen Maßnahmen mit Maßnahmen zu kombinieren, die das Mitarbeiterverhalten fokussieren (Hagen et al., 2008, S. 393). Im Mittelpunkt dieser Maßnahmen steht, die Aufmerksamkeit der Mitarbeiter auf das Thema Informationssicherheit zu lenken. Hierdurch kann erreicht werden, dass sich

die Mitarbeiter mehr mit dem Thema auseinandersetzen. Als Beispiel für eine solche Maßnahme lässt sich ein speziell entwickeltes Training anführen. Bereits 53% der Unternehmen führen laut einer Umfrage Maßnahmen durch, um die Aufmerksamkeit ihrer Mitarbeiter zu erhöhen (Gefahrenbarometer, 2010, S. 9). Durch dieses kann das Wissen der Mitarbeiter erhöht werden, wodurch nachweislich das Risiko für die Unternehmensdaten reduziert werden kann (Thompsen et al., 1994, S. 167). Hieraus lässt sich ableiten, dass nur eine Kombination aus technischen und personenbezogenen Sicherheitsmaßnahmen die Informationssicherheit sicherstellen kann, da es sonst zu Fehlinterpretationen oder Missverständnissen kommen kann (Siponen, 2000(b), S. 31). Um das Wissen der Mitarbeiter zu erhöhen verwenden Unternehmen verschiedene Maßnahmen. Zwei häufig verwendete sind hierbei Sicherheitspräsentationen und E-Learnings. Um herauszufinden, welche der beiden Methoden effektiver ist und sich somit besser eignet, um Mitarbeiter zu schulen, wird innerhalb dieser Arbeit ein Experiment durchgeführt, welches in den folgenden Kapiteln näher beschrieben wird.

Um einen besseren Überblick über das Thema Informationssicherheit zu erhalten, wurde bereits in einer früheren Arbeit eine Literaturanalyse durchgeführt. Es wurden zunächst, durch einen zuvor festgelegten Suchprozess, Veröffentlichungen ermittelt, die als Forschungsmethode Experimente verwendet haben. Hierdurch konnten 14 Artikel identifiziert werden. Nach näherer Betrachtung der Veröffentlichungen wurde festgestellt, dass 9 dieser hauptsächlich Studenten als Probandengruppe verwendet haben. Ziel von Forschern ist es oftmals, die Ergebnisse eines Experiments, die durch eine ausgewählte Probandengruppe entstanden sind, auf eine größere Gruppe zu verallgemeinern (Aronson et al., 2004, S. 48). Als Beispiel hierfür lässt sich die Veröffentlichung von Shaw et al. (2008) anführen. Ihr Forschungsziel war es, das Verhalten von Mitarbeitern zu untersuchen. Allerdings haben an dem Experiment nur Studenten teilgenommen. Dieses ist sehr problematisch, da Ergebnisse eines Experiments laut Definition dieser Methode nur auf gleiche Situationen generalisiert werden dürfen (Wellenreuther, 2000, S. 394). Andere Forscher, wie bspw. Johnston und Warkentin (2010, S. 563), haben ihre Ergebnisse aus diesem Grund im Ausmaß der Generalisierbarkeit eingeschränkt. Sie haben in ihren Limitationen beschrieben, dass die Ergebnisse nur in einem universitären Umfeld Gültigkeit haben, da sie ihr Experiment auch nur in diesen Bereich durchgeführt haben. Durch diese zwei Vorge-

hensweisen lässt sich die Frage stellen, ob es einen Unterschied zwischen dem Verhalten von jüngeren und älteren Personen in Bezug auf die Informationssicherheit gibt. Auf Grundlage der zuvor beschriebenen Probleme wurde die Forschungsfrage entwickelt:

** Gibt es Unterschiede zwischen dem Einfluss eines E-Learnings und dem Einfluss einer Präsenzveranstaltung auf das Informationssicherheitsverhalten von Mitarbeitern?*

Um diese Forschungsfrage beantworten zu können, wird im Rahmen dieser Arbeit ein Feldexperiment entwickelt. Dieses Experiment wird in einem internationalen Industrieunternehmen mit Hauptsitz in Deutschland durchgeführt. Alle Probanden des Experiments werden in Deutschland beschäftigte Mitarbeiter des Unternehmens sein. Die Angestellten werden in zwei Gruppen eingeteilt und nehmen an unterschiedlichen Schulungsmaßnahmen zur Erhöhung ihrer Aufmerksamkeit und ihres Wissens hinsichtlich des Themas Informationssicherheit teil. Damit eine Vergleichbarkeit der Schulungsmaßnahmen möglich ist, werden die Mitarbeiter gebeten, jeweils vor und nach der Schulungsteilnahme, an einer Umfrage teilzunehmen. Die zwei Umfragebögen bestehen aus den gleichen Basisfragen. Der einzige Unterschied besteht darin, dass der zweite Umfragebogen um zusätzliche Fragen zu der Schulungsmethode erweitert ist. Hierdurch kann die Qualität der Schulungsmaßnahme identifiziert werden. Nachdem die Umfragen von den Schulungsteilnehmern ausgefüllt worden sind, werden die Daten mit den Programmen SPSS und SmartPLS analysiert. Hierzu werden die Daten der ersten und zweiten Umfrage getrennt ausgewertet. Des Weiteren werden aus jedem Umfragebereich Mittelwerte gebildet und verglichen, wie sich diese durch die Schulungsmaßnahmen verändert haben. Anschließend wird in dieser Arbeit das Ergebnis des Experiments diskutiert und Handlungsempfehlungen für die Praxis und den akademischen Bereich gegeben. Außerdem werden zum Ende der Arbeit die Limitationen dieses Experiments beschrieben und ein abschließendes Fazit gezogen.

speichert (Jenkins et al., 2012, S. 3289). In diesem Fall wurden die Einstellung und die Verhaltensabsicht der Mitarbeiter direkt nach der Schulungsmaßnahme abgefragt. Dieses ist auf die zeitliche Begrenzung der Forschungsarbeit zurückzuführen. Um die Wirkungsweise der jeweiligen Schulungsmaßnahme auf einen längeren Zeitraum und damit auch das abgespeicherte Wissen im Langzeitgedächtnis analysieren zu können, müsste der Zeitraum zwischen der Schulungsmaßnahme und der zweiten Umfrage größer sein. Hierbei wäre es dann auch möglich zu untersuchen, ob die Sicherheitsvorfälle durch die Schulungsmaßnahme reduziert werden konnten. Außerdem könnte in einer Langzeitstudie analysiert werden, in welchen zeitlichen Abständen die Schulungen wiederholt werden sollten, um die Informationssicherheit im Unternehmen zu gewährleisten (Hagen und Albrechtsen, 2009, S. 398). Die Schulung wurde mit Hilfe von Focus Areas strukturiert. Jeder Mitarbeiter wurde seinem Nutzer-Profil zugeordnet. In diesem Experiment wurden 3 Nutzer-Profile verwendet. Um jedoch die Aufmerksamkeit der Mitarbeiter möglichst lange aufrecht zu erhalten, sollten Nutzer-Profile in kleinere Unterkategorien untergliedert werden. Hierdurch könnte hinzukommend erreicht werden, dass die Mitarbeiter nur so viel Arbeitszeit wie nötig verwenden, um die Schulung zu absolvieren. Außerdem wurde ermittelt, dass die Benutzerfreundlichkeit und das empfundene Vergnügen des Web-Based-Trainings im Vergleich zu der Präsenzschulung gering ausgefallen sind. Dieses ist darauf zurückzuführen, dass die Schulung nur wenig Interaktion enthielt. Aufgrund dieses Qualitätsmerkmals ist es möglich, dass die Ergebnisse bei einer erneuten Durchführung des Experiments, mit einem anders gestalteten Web-Based-Training, verändert ausfallen.

8. Fazit

Die vorangegangenen Kapitel haben unter anderem die Vor- und Nachteile von Web-Based-Trainings und Präsenzschulungen aufgezeigt. Präsenzschulungen werden schon sehr lange verwendet um Personen zu schulen. In den letzten zehn Jahren wurden aber auch Web-Based-Trainings immer häufiger zu Schulungszwecken verwendet (Zhou, 2013, S. 664). Ein Grund für die sinkende Verwendung von Präsenzschulungen ist die Ortsgebundenheit der beteiligten Personen. Sowohl der Schulungsleiter als auch die Schulungsteilnehmer müssen sich zu einem bestimmten

Zeitpunkt an dem gleichen Ort zusammenfinden. Hierdurch entstehen Kosten und der zeitliche Aufwand ist für die Beteiligten sehr groß (Rozewski, 2011, S. 23). Als weiterer Vorteil des Web-Based-Trainings kann die Individualität angesehen werden. Es ist möglich, die Schulung so zu konzipieren, dass sie mit dem Vorwissen, den Fähigkeiten und der Einstellung des Teilnehmers abgestimmt sind. Somit ist ein Web-Based-Training an jeden Typ von Mitarbeiter anpassbar (Zhou, 2013, S. 668). Innerhalb dieses Experiments wurden auch verschiedene Nutzer-Typen von Mitarbeitern erstellt. Hierzu wurden Focus Areas genutzt, die die wichtigsten Bereiche der Informationssicherheit beschreiben. Je nach Aufgabengebiet und IT-Nutzung eines Mitarbeiters wurden ihm Focus Areas zugeteilt. Hierdurch haben die Mitarbeiter nur das Wissen vermittelt bekommen, dass für ihre Tätigkeiten wichtig ist. Durch dieses Vorgehen sollte verhindert werden, dass Mitarbeiter Schulungsinhalte vermittelt bekommen, die sie nicht benötigen. Dieses ist von Vorteil, da Schulungen möglichst auf die wichtigsten Inhalte reduziert werden sollten, damit die Konzentration erhalten bleibt (Thomson und Solms, 1998, S. 172).

Weiterhin sind in dieser Arbeit der Aufbau und die Durchführung des Experiments beschrieben. Es wurde entschieden, ein Feldexperiment durchzuführen, da dieses einige Vorteile gegenüber einem Laborexperiment aufweist. Durch die Integration des Experiments in eine reale Umgebung ist es möglich, die Ergebnisse auf eine größere Personenanzahl zu generalisieren (Häder, 2010, S. 341). Trotz dieses Vorteils mussten in den Limitationen einige Eingrenzungen gesetzt werden. Das Experiment wurde in einem deutschen Unternehmen für Antriebstechnik und Automation durchgeführt. Durch diese Tätigkeit gehört das Unternehmen der Maschinenbaubranche an. Da jede Branche kulturelle Besonderheiten aufweist, ist es nur möglich die Ergebnisse auf Maschinenbauunternehmen in Deutschland zu generalisieren. Da diese Branche allerdings einer der größten Arbeitgeber in Deutschland ist, ist es trotzdem möglich, auf das Informationssicherheitsverhalten von über 5,2 Millionen Arbeitnehmern zu schließen (Bundesministerium für Wirtschaft und Energie, 2014). Aufgrund der Tatsache, dass Deutschland der viertgrößte Industriestandort der Welt ist, ist die Branche nicht nur ein wichtiger Arbeitgeber, sondern auch für einen großen Teil der deutschen Wirtschaftsleistung verantwortlich. Besonders die starke Position Deutschlands auf dem Weltmarkt führt dazu, dass Industrieunternehmen hierzulande großen Gefahren durch Industriespionage ausgesetzt sind. Aus diesem

Grund müssen besonders deutsche Unternehmen einen großen Wert auf die Informationssicherheit legen, um ihr spezialisiertes Wissen vor Manipulation oder Verlust zu schützen (Fussan, 2010, S. 259).

Das Experiment wurde im Zeitraum Februar 2014 bis September 2014 in dem beschriebenen Unternehmen durchgeführt. Hierzu wurde ein sechsmonatiges Praktikum absolviert, in welchem zum einen die Schulungen entwickelt und durchgeführt wurden und zum anderen die Daten erhoben und analysiert worden sind. Die Daten wurden mithilfe eines selbst entwickelten Fragebogens erhoben und es konnten durch die Analyse die folgenden Ergebnisse festgestellt werden. Es konnte bestätigt werden, dass Schulungen im Bereich der Informationssicherheit zu einer positiven Veränderung der Verhaltensabsicht führen. Durch die Teilnahme an einer der Schulungsarten haben die durchschnittlichen Werte aller Konstrukte des Forschungsmodells zugenommen. Somit haben die Teilnehmer nach der Schulungsteilnahme die Bedrohungen schwerwiegender eingeschätzt und ihre Bewältigungsmöglichkeiten der Bedrohungen besser wahrgenommen. Außerdem haben sich die Werte der Nützlichkeit und der Benutzerfreundlichkeit der Sicherheitsrichtlinien nach der Schulungsteilnahme positiv verändert. Weiterhin konnte festgestellt werden, dass sich die Einstellung zu den Sicherheitsrichtlinien verbessert hat, welches einen direkten Einfluss auf die Verhaltensabsicht der Personen hat. Auf der anderen Seite konnte allerdings nicht bestätigt werden, dass ein Web-Based-Training eine wirkungsvollere Schulungsart ist, um Personen im Bereich der Informationssicherheit weiterzubilden. Jedoch konnte ermittelt werden, dass insbesondere jüngere Menschen dazu neigen, an einem Web-Based-Training teilzunehmen, da die Teilnehmerzahlen der jungen Personen bei dem Web-Based-Training wesentlich höher ausfallen als die Teilnehmerzahlen der jüngeren Personen bei der Präsenzschulung. Des Weiteren haben jüngere Personen die Schulungsart des Web-Based-Trainings nützlicher bewertet, als Personen der älteren Altersklassen. Aus diesem Grund sollten Web-Based-Trainings stetig weiterentwickelt werden, um die Nachfrage nach einer zeitunabhängigen Schulungsart zu bedienen.

Bei zukünftigen Forschungen sollte insbesondere der Langzeiteffekt von den verschiedenen Schulungsmethoden untersucht werden. Hierbei wäre es insbesondere interessant zu erforschen, in welchen Abständen die Schulungen wiederholt werden

müssten, damit die Informationssicherheit der Unternehmensdaten gewährleistet werden kann. Außerdem sollten die Teilnehmer des Experiments aus verschiedenen Ländern und Branchen stammen. Hierdurch kann der kulturelle Einfluss auf die Ergebnisse möglichst gering gehalten werden. Weiterhin sollten die Stichprobengrößen einheitlich gewählt werden, damit die Vergleichbarkeit der verschiedenen Umfragen möglichst groß ist. Bei der Entwicklung der Schulungen sollte beachtete werden, die Schulungstypen in möglichst kleine Unterkategorien zu unterteilen. Somit erhält jeder Mitarbeiter nur das für ihn notwenige Wissen. Durch dieses Vorgehen kann gewährleistet werden, dass die Mitarbeiter die Informationen bestmöglich aufnehmen und nur so viel Zeit wie notwendig aufbringen, um die Schulung zu absolvieren.