Stärkung des IT-Sicherheitsbewusstseins im Rahmen des IT-Risikomanagements

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der

Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Uffen Vorname: Jörg

[redacted]

Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, den 13. Januar 2009

Vorwort

An dieser Stelle möchte ich all denjenigen meinen Dank aussprechen, die mich bei der Erstellung der vorliegenden Arbeit mit Informationen und Anregungen unterstützt haben.

Mein Dank geht in erster Linie an Herrn Prof. Dr. Michael H. Breitner, der mir bei der Erarbeitung sowie bei der Wahl des Themas völlige Freiheiten ließ und mich stets mit Anregungen motivierend unterstützt hat.

Besonderen Dank möchte ich Frau Dr. Claudia M. König aussprechen – sie hat sich sehr viel Zeit für die Unterstützung meiner Arbeit genommen und mir geduldig mit fachlichen Hinweisen und Ratschlägen aus der Psychologie sowie der Pädagogik zur Seite gestanden. Mir ist bewusst, dass eine derartig gute Betreuung keine Selbstverständlichkeit ist.

Ein herzliches Dankeschön geht an meinen ehemaligen Arbeitskollegen und guten Freund Florian Madertoner für seine guten Deutschkenntnisse (bzw. Österreichischkenntnisse) und sein besonderes Engagement bei der Umschiffung so mancher sprachlicher Barriere.

Ein weiterer Dank gilt meinem guten Freund Hermann Ossowski, der mir ebenfalls bei meiner Arbeit mit Rat und Tat zur Seite stand und immer ein offenes Ohr hatte.

Nicht zuletzt möchte ich mich bei allen Teilnehmern bedanken, die sich im Rahmen der Experteninterviews, trotz meist zeitlicher Engpässe, breitwillig engagiert haben.

Weiterhin möchte ich mich bei Allen bedanken, die sich täglich in der Bibliothek einen Gruppenraum mit mir geteilt haben und es mir erleichtert haben, Zwischentiefs und Motivationslöcher leichter zu überwinden.

Jörg Uffen

Inhaltsverzeichnis

Vorwort ... II

Inhaltsverzeichnis ... III

Tabellenverzeichnis ... VII

Abkürzungsverzeichnis ... VIII

1. Einleitung ... 1

1.1 Problemstellung und Motivation ... 1

1.2 Aufbau der Arbeit ... 2

2. Theoretische Grundlagen ... 3

2.1 Risiken eines Unternehmens ... 3

2.1.1 Klassifikation der Unternehmensrisiken ... 4

2.1.2 IT-Risiken ... 6

2.2 Stellenwert von Informationen ... 10

2.3 IT-Sicherheit innerhalb von Organisationen ... 12

2.3.1 Die Schutzziele der IT-Sicherheit ... 13

2.3.2 Personelle IT-Sicherheit – Sicherheitsbewusstsein ... 17

2.4 Risikomanagementprozess ... 18

2.4.1 Risikoidentifikation ... 18

2.4.2 Risikobewertung ... 19

2.4.3 Risikosteuerung ... 20

2.4.4 Risikokontrolle ... 20

3. Regulatorische Einflüsse ... 21

3.1 KonTraG ... 21

3.2 GoBS ... 22

3.3 Sarbanes Oxley Act ... 23

3.4 Regelungen im Strafgesetzbuch ... 23

3.5 Haftung von Mitarbeitern ... **24**

4. Lösungsansätze zur Vermeidung insiderorientierter Risiken ... **25**

4.1 Pädagogische Wissensteuerung ... **25**

4.1.1 Erhebung einer Lernkultur ... 25

4.1.2 Lerntheorien im Überblick ... 27

4.1.3 Richtungsweisende anreizbasierte Motivationsgrundlagen ... 32

4.1.4 Anreize in der Motivationstheorie ... 36

4.1.5 Organisationskultur ... 39

4.1.6 Werte und Normen ... 44

4.1.7 Artefakte ... 44

5. Sensibilisierungskampagne als Risikoreduzierungsmaßnahme zur Sicherung der IT-Sicherheit ... **45**

5.1 Motive und Faktoren für fehlendes Sicherheitsbewusstsein auf der Mitarbeiterebene **45**

5.2 Exemplarische Schadensfälle durch Innentäter ... **48**

6. Handlungsempfehlungen zur nachhaltigen Mitarbeitersensitiven Umsetzung von IT-Sicherheit – ein 5-Phasen Modell ... **51**

6.1 Grundphase – Grundvoraussetzungen schaffen ... **51**

6.1.1 Anforderungen an das Management ... 51

6.1.2 Berücksichtigung kultureller Unterschiede im multinationalen Umfeld ... 54

6.1.3 Der Grundstein zum Erfolg – eine ausgebildete Sicherheitskultur ... 55

6.2 Phase 2 – Diagnose ... **60**

6.2.1 Ausgewählte Standards und Best-Practices zu mehr IT-Sicherheitsbewusstsein ... 60

6.2.2 Der Status Quo des Security Awareness ... 63

6.2.3 Einstufung von Risiken ... 69

6.2.4 Zielgruppenanalyse ... 72

6.3 Phase 3 – Design einer effektiven Kampagne ... **76**

6.3.1 Grundlegender Aufbau der Lernziele ... 76

6.3.2 Auswahl der Lernkanäle ... 82

6.4 Phase 4 – Umsetzung des Security Awareness Trainings ... **88**

6.5 Phase 5 – Evaluierung und Verbesserung ... **92**

6.5.1 Kontrollphase ... 92

6.5.2 Verbesserung ... 98

6.6 Security Awareness Kampagnen in der Praxis ... **102**

6.7 Explorative Experteninterviews ... **104**

6.7.1 Methodik und Gesprächspartner ... 104

6.7.2 Security Awareness aus Expertensicht ... 105

7. Fazit und Ausblick ... **113**

Literaturverzeichnis ... **118**

Anhang 1: Fragebogen zur telefonischen Expertenbefragung ... **136**

Anhang 2: Fragebogen zur Expertenbefragung per E-Mail ... **138**

Erklärung ... **141**

1. Einleitung

1.1 Problemstellung und Motivation

Im Laufe der letzten Jahre fand eine konsequente Wandlung von der Industriegesellschaft hin zu einer Informationsgesellschaft statt. Grund für diese Entwicklung ist die zunehmende Bedeutung von Wissen und Informationen für den Erfolg und die Wettbewerbsfähigkeit jedes Unternehmens[1]. Neben den klassischen Produktionsfaktoren Arbeit, Boden und Kapital hat sich zunehmend der Faktor Informationen und Wissen etabliert. Nahezu alle Geschäftsprozesse werden in der heutigen Gesellschaft von Informationen, Wissen und Kommunikation beeinflusst. Auf Grund dessen kann durch den intelligenten Einsatz der Informations- und Kommunikationstechnologie innerhalb eines Unternehmens die Wettbewerbsfähigkeit beträchtlich gesteigert werden[2].

Informationen sind somit als Erfolgsfaktor ein schützenswertes Gut. Die Verarbeitung und Speicherung eines Großteils der Unternehmensinformationen wie z. B. Rechnungen, Briefen oder Präsentationen erfolgt in elektronischer Form. Diesbezüglich kommt der Informationstechnik (kurz: IT) eine Schlüsselfunktion u.a. für das Informationsmanagement als auch für die Informationssicherheit zu[3]. Allerdings liegt genau in diesem Punkt die eigentliche Problematik. Durch das Internet-basierte World-Wide-Web und die zunehmend wachsende Zahl von Mediendiensten sehen sich Unternehmen einer in den letzten Jahren exponentiell steigenden Zahl an Bedrohungen gegenüber. Viren und Würmer verbreiten sich meist über den Missbrauch von mit dem Internet verbundenen PCs in kürzester Zeit flutartig und infizieren ein gesamtes betriebliches IT-System[4]. Die steigende Quantität und Qualität der Angriffe auf betriebliche IT-Systeme erfordern somit zunehmend schnellere und komplexere Gegenmaßnahmen[5].

Nahezu jedes Unternehmen verfügt über technische Einrichtungen, wie Virenscanner und Firewalls, die bei systematischer Aktualisierung und geeigneter Konfiguration den größten Ansturm überwiegend Stand hielten[6]. Hierfür wurden teils horrende Summen für das Errichten elektronischer Schutzmechanismen investiert, um sensible Daten gegen Diebstahl,

[1] vgl. Wirtz/ Sammerl (2003), S. 83
[2] vgl. Schmidt (2006), S. 1
[3] vgl. Schmidt (2006), S. 4
[4] vgl. Fox/ Kaun (2005), S. 329
[5] vgl. Hartmann (2008), S. 35
[6] vgl. Fox/ Kaun (2005), S. 329

Manipulation oder Verlust zu schützen[7]. Verursachte Schäden gehen allerdings meist nicht von Fehlern in Scannern oder Firewalls aus, sondern werden von den eigenen Mitarbeitern verursacht, die bspw. über ihre Notebooks schadenstiftende Software in das betriebsinterne Netz einschleusen[8]. Unter Berücksichtigung der 80-20 Regel, nach der 80% aller Sicherheitsvorfälle durch menschliches Versagen und nur 20% durch technisches Versagen verursacht werden, liegt ein großes ungenutztes Sicherheitspotenzial beim Menschen[9]. Die Anforderungen an die Nutzer steigen somit mit rasanter Geschwindigkeit[10]. Virenscanner und Firewalls können nur bekannte Angriffe abwehren, während ein sensibilisierter Mensch auch potenzielle unbekannte Attacken prognostizieren, mit seinem Wissen abgleichen und entsprechende Gegenmaßnahmen einleiten kann.

Die Ursachen für menschliches Fehlverhalten sind bspw. durch die wiederkehrenden Ergebnisse der <kes>-Sicherheitsstudien bereits mehrfach bestätigt worden und liegen in Nachlässigkeiten, Irrtum, Gewohnheiten und Unkenntnis[11]. Diese Risikofaktoren gilt es durch ein umfassendes Risikomanagement zu identifizieren und auf ein akzeptables Maß zu reduzieren. Als besonders wirkungsvoll erweisen sich vor allem umfassende Sicherheitsbewusstseinskampagnen, bei der eingehend Sicherheitslücken geschlossen werden sollen. Die Konzeption einer effektiven Kampagne erweist sich allerdings als nicht sehr einfach, denn der Faktor Mensch zeugt von immenser Komplexität. Um menschliche Verhaltensweisen gezielt lenken zu können, müssen tief greifende Erkenntnisse des menschlichen Wesens, seines Handelns und der Motivation, sowie seiner lernenden Fähigkeiten berücksichtigt und in eine Kampagne wirkungsvoll integriert werden.

Von besonderer Wichtigkeit spricht die Schaffung einer begrifflichen Grundlage, um aus deren Erkenntnissen konkrete praktische Handlungsempfehlungen ableiten zu können.

1.2 Aufbau der Arbeit

Die nachfolgende Abbildung visualisiert den Aufbau der Arbeit:

[7] vgl. Eichler (2007), S. 92
[8] vgl. Fox/ Kaun (2005), S. 329
[9] vgl. Schlienger (2006), S. 1
[10] vgl. Hartmann (2007), S. 35
[11] vgl. <kes>/ Microsoft (2008), S. 18ff.

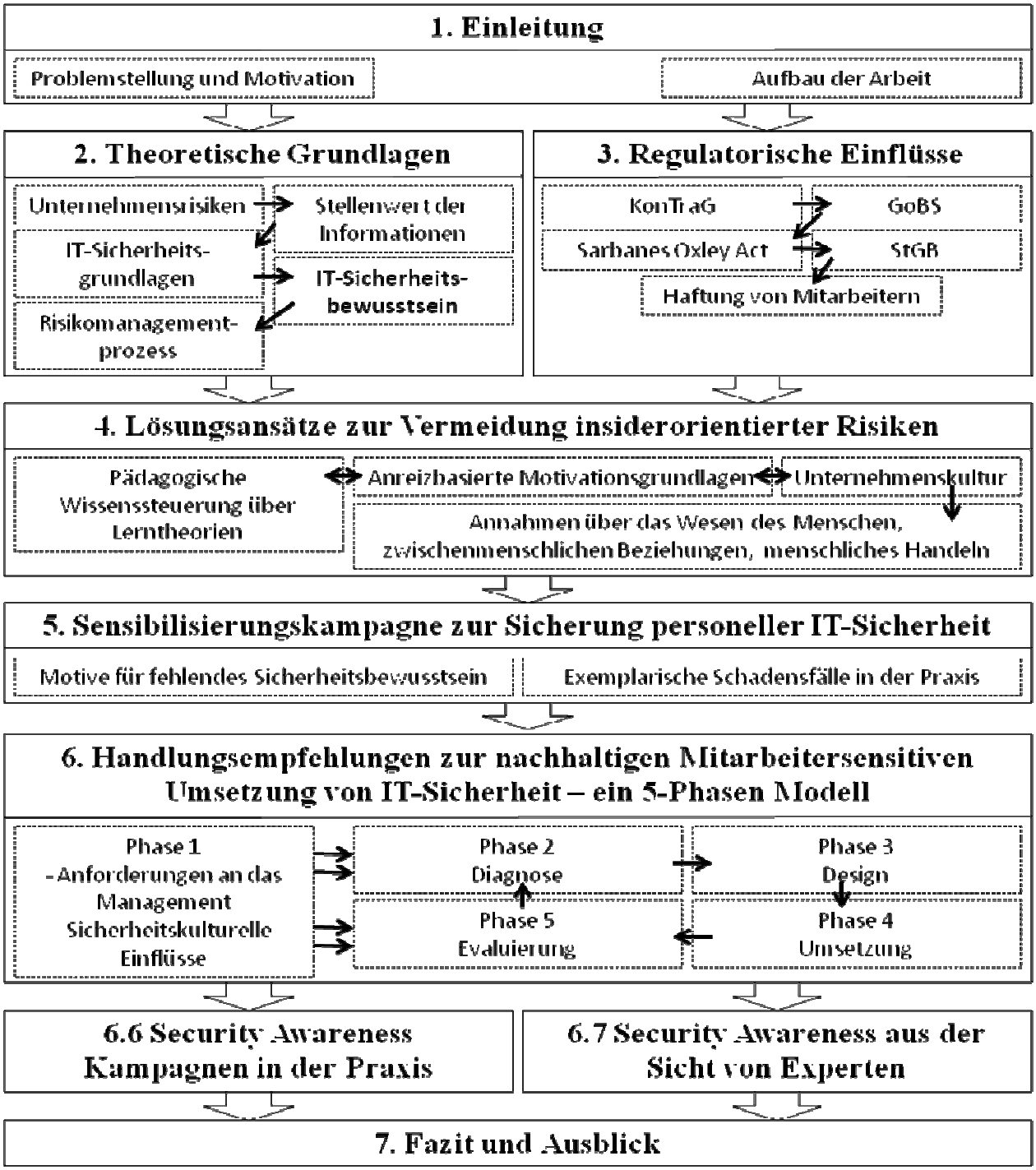

Abb. 1 Aufbau der Arbeit

Quelle: eigene Darstellung

2. Theoretische Grundlagen

2.1 Risiken eines Unternehmens

Das Eingehen von Risiken ist in der ökonomischen Geschäftstätigkeit eines Unternehmens unumgänglich geworden. Risiken bergen die Gefahr, dass durch interne oder externe Ereig-

der Wissensvermittlung. Da Lernen als individueller Prozess stattfindet, muss auch jeder Lernende die Möglichkeit haben, anhand verschiedener individuell präferierter Medien Wissen zu generieren[411].

Ein weiteres zu erwartendes unstimmiges Ergebnis wurde bei der Frage nach Kontrollmaßnahmen erzielt. Demnach bewerteten jeweils 30% der Probanden den Einsatz von gezielten Kontrollmaßnahmen nach der Durchführung einer Schulung als „sehr wichtig“ bzw. als „wichtig“. Auf der anderen Seite hielten 10% Kontrollmaßnahmen für „weniger wichtig“ sowie 30% für „überhaupt nicht wichtig“. Kontrollen zielen auf das Prinzip der Minderung eines spezifischen Verhaltens ab und sind in der Praxis nicht unumstritten. Kontrollmaßnahmen können zu einer Demotivation und einer verminderten Identifikation mit dem Unternehmen führen, auf der anderen Seite allerdings auch das Gegenteil bewirken und als Anreiz eingesetzt werden. Aus diesem Grund sind Kontrollmaßnahmen mit Vorsicht einzusetzen, sodass sich keine negativen Auswirkungen einfinden. Es gilt die richtige Balance zwischen den vom Mitarbeiter als zu negativ eingestuften und den vom Unternehmen als für notwendig empfundenen Kontrollen zu finden.

Einigkeit herrschte allerdings wieder bei der Frage nach der Wichtigkeit der Einleitung von Sanktionen im Falle von fahrlässigem Verhalten. Demzufolge hielten 20% der befragten Experten den Einsatz als „sehr wichtig“ während weitere 70% dies als „wichtig“ einstuften. Konsequentes Durchgreifen ist somit ein entscheidender Faktor, um fahrlässiges Verhalten internalisieren zu können.

Durch die Expertenbefragung konnten viele der erarbeiteten Erkenntnisse bestätigt und weiter ausgeführt werden. Erstaunliche Ergebnisse wurden vor allem im Rahmen der Effektivitätsmessung erzielt, die in Unternehmen auf Grund von zu geringen Budgets häufig ausbleibt. Dass dies die Effektivität einer Kampagne wesentlich einschränken kann, da Sicherheitslücken verbleiben können, wird dabei vielfach leider unterschätzt.

7. Fazit und Ausblick

Als Ausgangspunkt für die Betrachtung einer umfassenden Kampagne zur nachhaltigen Generierung von Sicherheitsbewusstsein wurden zu Beginn der Arbeit theoretische Grundlagen dargestellt, um aus deren Erkenntnissen konkrete Handlungsempfehlungen ableiten zu

[411] vgl. Kap. 6.3.2

können. Um Informationen, Daten oder schutzwürdige Belange nachhaltig zu schützen, müssen sämtliche Risiken erkannt, beurteilt und auf ein akzeptables Maß reduziert werden. Fälschlicherweise wird innerhalb einer Organisation häufig lediglich in technische Komponenten wie Virenscanner oder Firewalls investiert und weniger in die Ausbildung von Sicherheitsbewusstsein der Mitarbeiter, um die Grundeigenschaften der IT zu sichern. Sicherheitsbewusstes Handeln führt zu einer gedanklichen Reflexion eines Mitarbeiters über potenzielle Risiken, die sich im Umgang mit der IT im täglichen Arbeitsprozess ergeben können.

Dementsprechend wird dem Menschen ein bedeutender Stellenwert im Rahmen des Risikomanagements zugesprochen. Durch die Darstellung der regulativen Einflüsse, denen sich Unternehmen und auch Mitarbeiter zunehmend stellen müssen, konnte dies weiter unterstrichen werden.

Die Internalisierung des Faktors Mensch im Rahmen einer umfassenden Security Awareness Kampagne zeugt von hoher Komplexität und Interdisziplinarität. So mussten Elemente der Pädagogik, Didaktik, Organisationspsychologie sowie Personalwirtschaftslehre dargestellt und anschließend in die Kampagne integriert werden. Mittels der drei Lernparadigmen des Behaviorismus, Kognitivismus und Konstruktivismus wurden ausgewählte Ansätze dargestellt, die das menschliche Lernen näher konkretisieren. Klargestellt wurde, dass dabei keine Fokussierung auf ein einzelnes Paradigma möglich war. Vielmehr wurden jeweilige Elemente der Paradigmen mit in die Kampagne integriert, um durch Vielseitigkeit die individuellen Präferenzen des Lernens jedes Mitarbeiters ansprechen zu können.

Die Wissensgenerierung allein muss allerdings noch nicht in einer tatsächlichen sicherheitskonformen Verhaltensänderung münden. Aus diesem Grund wurde auf Ansätze der anreizbasierten Motivationstheorie zurückgegriffen, dessen Elemente in Abstimmung mit dem jeweilig in einem Unternehmen vorherrschendem Menschenbild Einzug finden mussten. Menschenbilder stellen ein wichtiges Element der Unternehmenskultur dar. Nach der Theorie pluralistischer Menschenbilder, deren Vertreter u.a. Edgar Schein ist, wird der Mensch heute als komplexes Wesen („complex man“) gesehen, der äußerst wandlungs- und anpassungsfähig ist. Auf Grund erfahrungsbedingter, ständiger Änderungen der Motive müssen auf Unternehmensebene individuelle auf den Mitarbeiter bezogene Anreize gesetzt werden.

Die eigentliche Kampagne wurde anhand eines 5-Phasen Modells entwickelt. Mit der ersten Phase wurden Grundvoraussetzungen geschaffen, die für eine umfassende Kampagne unabdingbar sind. Zu diesen zählt vor allem der Faktor des Management-Supports, der sich

durch die gesamte Kampagne ziehen muss. Das Management muss nicht nur eine Vorbildfunktion durch richtige Verhaltensweisen für alle Beschäftigten einnehmen, sondern weiterhin durch eine aktive Anteilnahme auf die Bedeutsamkeit von Sicherheitsmaßnahmen innerhalb einer Organisation hinweisen.

Ein weiterer wichtiger Faktor dieser Phase lag in einer ausgebildeten Sicherheitskultur, als zentrales Element der Unternehmenskultur. Im Zuge einer Security Awareness Kampagne müssen nicht nur kulturelle Unterschiede Berücksichtigung finden, sondern vielmehr müssen für den Mitarbeiter sichtbare, leicht identifizierbare Teile der Unternehmenskultur gezielt verändert werden. Weiterhin sind auch teilweise sichtbare und unsichtbare Elemente einer Unternehmenskultur bereits im Vorfeld zu identifizieren und in den Phasen der Kampagne zu berücksichtigen. Eine Security Awareness Kampagne führt somit nicht nur zu einer Veränderung der Unternehmenskultur, sondern auch die Kultur an sich beeinflusst die Kernpunkte der Herangehensweise einer Kampagne. Im Grunde genommen kann im Rahmen einer ausgebildeten Sicherheitskultur nicht von einer einzelnen Phase gesprochen werden. Vielmehr gehen alle Fäden der Herangehensweise einer Kampagne von den Werten und Normen der Unternehmenskultur aus. Somit besteht auch ein Einfluss auf das Management. Allerdings sind bestimmte Elemente für die Erreichung der Ziele gezielt zu verändern. Demnach kann bspw. keine Gruppenarbeit ausgeführt werden, wenn innerhalb des Unternehmens eine schlechte zwischenmenschliche Beziehung besteht.

Durch die Phasen 2 bis 5 wurde das eigentliche Benutzertraining umfassend diskutiert. Begonnen wurde mit der Diagnosephase, bei der zunächst der Ist-Zustand ermittelt, eine Risikoeinteilung vorgenommen sowie eine Zielgruppenanalyse vollzogen wurde. Diese Phase ist eine der Bedeutendsten, denn anhand der Ergebnisse vollzieht sich der gesamte Weg der Kampagne. Im Anschluss hieran erfolgte die Konstruktion der Designphase, bei der durch einen Soll-Ist-Vergleich die Lerninhalte festgelegt und die Lernkanäle ausgewählt wurden.

Das eigentliche Training wurde durch die Phase 3 umgesetzt. In diesem Zusammenhang wurden die erarbeiteten Erkenntnisse der vorherigen Phasen in das Benutzertraining eingebettet und entsprechend umgesetzt. Beispielhaft wurde ein Benutzertraining konstruiert, welches neben dem Einsatz von E-Learning Modulen auch auf eine Präsenzschulung baute, bei der jeweils die verschiedenen Ansätze des Lernens berücksichtigt wurden.

In der letzten Phase der Kampagne, der Evaluationsphase, wurden ausgewählte Maßnahmen erläutert, mit denen die Wirksamkeit einer Kampagne überprüft werden sollte. Herausgestellt hat sich jedoch, dass eine reine Wissensabfrage keine reale Verhaltensänderung bewirken

muss. Vielmehr galt es auch, tatsächliche Verhaltensweisen zu beobachten. Die diskutierten Methoden erwiesen sich für die praktische Anwendung auf Grund ihrer hohen Komplexität als tendenziell unvorteilhaft und würden die in der Praxis ohnehin bereits begrenzten Budgets sicherlich sprengen.
Um Nachhaltigkeit erhalten zu können, wurde weiterhin auf den Aspekt der Verbesserung eingegangen, die dem Mitarbeiter als „Gedankenstütze" dienen soll. Hierbei wurden verschiedene Möglichkeiten dargestellt, die jeden Beschäftigten kontinuierlich im Arbeitsprozess an die Einhaltung der Sicherheitsmaßnahmen erinnern soll.

In Anlehnung an den Annahmen des „complex man" wurden durch die gesamten Phasen hinweg möglichst breite Anreize gesetzt, um jeden Mitarbeiter individuell ansprechen zu können. Weiterhin wurde der Aspekt der Identifikation mit einem Unternehmen besonders hervorgehoben. Dadurch, dass in den ersten Phasen nur wenige Anreize gesetzt werden konnten, später allerdings vermehrt verschiedene Anreize eingesetzt wurden, wurde davon ausgegangen, dass das Motivationsniveau der Mitarbeiter bis zur Umsetzung des Trainings kontinuierlich steigen würde. In der Kontrollphase musste es durch die beschriebenen Verbesserungsprozesse auf ein möglichst konstantes Niveau gehalten werden. Erst dadurch ist die Einhaltung sicherheitskonformer Verhaltensweisen gewährleistet.
Mittels empirischer Studien wurden durch die gesamte Arbeit hinweg zahlreiche Belege für die beschriebenen Vorgehensweisen gegeben.
Eine Veranschaulichung von Security Awareness Kampagnen in der Praxis wurde durch die Beispiele von T-Systems sowie der Münchener Rück gegeben. Diese Unternehmen hatten in den vergangenen Jahren bereits interessante Kampagnen durchgeführt, wobei das Grundkonstrukt dieser Arbeit auffällig nahe war.
Zum Abschluss konnte anhand einer explorativen Expertenbefragung gezeigt werden, dass die erarbeiteten Elemente der Arbeit bedeutsam für eine Security Awareness Kampagne sind. Aus den Ergebnissen ließen sich weiterhin zahlreiche ergänzende Aussagen für eine nachhaltige Sicherheitsbewusstseinskampagne ermitteln. Dabei konnte bspw. festgestellt werden, dass die Hauptquelle für fehlendes Sicherheitsbewusstsein zum Einen in der Person des Mitarbeiters selber, zum Anderen aber auch im Management bzw. im Unternehmen liegen kann. Den Aussagen konnte auch entnommen werden, dass auch die sichtbaren Elemente einer Unternehmenskultur von ausschlaggebender Bedeutung für den Erfolg einer Kampagne sind. Ein Unternehmen, dass für mehr Sicherheit im Umgang mit der IT wirbt, auf der anderen

Seite aber Entlassungen und dadurch soziale Sicherungen bricht, wird wenig Glaubhaftigkeit bei den Mitarbeitern erzielen können.

Security Awareness ist nach wie vor ein viel diskutiertes Thema. Die letzten Monate und Jahre konnten vielerlei Beispiele aufzeigen, wie anfällig verschiedene Unternehmen für Datenmissbrauch oder Datendiebstahl waren bzw. sind. Dies wird jedes Unternehmen gleich welcher Größe zu einer Reaktion zwingen. Der Stellenwert von Sicherheitsbewusstsein innerhalb von Unternehmen wird somit vor allem in den nächsten Jahren weiter drastisch steigen.
Sicherheitsbewusstsein ist schon längst kein isoliertes Thema der Wirtschaftsinformatik mehr. Vielmehr werden auch in Zukunft weiter interdisziplinäre Ansätze die Thematik erforschen. Besonders psychologische und pädagogische Ansätze werden weiter gefragt sein, um den Menschen weiter berechenbar zu machen und seine Verhaltensweisen gezielt lenken zu können. Weiterhin wird auch die bislang häufig vernachlässigte Effektivitätsmessung eine bedeutende Rolle in der Forschung einnehmen. Denkbar wäre die Entwicklung von Tools, die eine sinnvolle Unterstützung der Ansätze nach Kruger/ Kearney liefern.
Nichts desto trotz wird sich das Thema Sicherheitsbewusstsein als einzelne Disziplin in der Forschung etablieren und niemals an Aktualität verlieren.

Wer sichere Schritte tun will, muss langsam gehen. (Johann Wolfgang von Goethe)