Der Mitarbeiter als Komponente der Informationssicherheit

Peter Roßbach

Wirtschaftsinformatik
Frankfurt School of Finance & Management
Sonnemannstraße 9-11
60314 Frankfurt
p.rossbach@fs.de

Abstract: In der Literatur zur Informationssicherheit existieren viele Beiträge, die sich mit der Frage befassen, welche Maßnahmen und Instrumente ein gewünschtes Verhalten bei den Mitarbeitern in Unternehmen bewirken können. Es fehlen jedoch Studien, die die ursächlichen Faktoren auf Einstellung und Verhalten untersuchen. Einen Beitrag dazu leistet diese Arbeit. Es werden sieben Faktoren herausgearbeitet und in ihrem Einfluss auf Einstellung und Verhaltensabsicht analysiert. Neben Wissen und Verantwortungsgefühl erweisen sich dabei vor allem die empfundene „Bequemlichkeit" sowie die Einschätzung der Wirksamkeit der Informationssicherheit im Unternehmen als wesentliche Einflussfaktoren. Eine getrennte Analyse nach der Teilnahme bzw. Nicht-Teilnahme an Awareness-Kampagnen zeigt zudem, dass diese sich positiv auf Einstellung und Verhaltensabsicht auswirken.

1 Einleitung

In der Forschung wie auch in der Praxis der Informationssicherheit wurde lange Zeit der Mensch im Unternehmen als Sicherheitskomponente vernachlässigt. Es fand zunächst eine Konzentration auf die Technik statt, die dann zunehmend um organisatorische Elemente erweitert wurde. Diese beiden Komponenten und ihr Zusammenspiel sind mittlerweile recht gut analysiert und in der Umsetzung ausgereift, weshalb in den vergangenen Jahren zunehmend der Mensch in den Fokus der Angreifer rückte.

Anders als bei den technischen Sicherheitssystemen handelt es sich beim Menschen nicht um einen starr die Sicherheitsvorschriften befolgenden Automaten, sondern er wird angetrieben von fachlichen sowie persönlichen Zielen und Motiven und hat die Einhaltung der Sicherheit nicht als primäre Aufgabe. Nachlässigkeit, Fehler und bewusste Sicherheitsverstöße (z.B. aufgrund von Zeitdruck) können erhebliche Folgen auf die Informationssicherheit haben und beinhalten somit ein beträchtliches Risikopotential. Viele Beispiele aktueller Angriffe auf Unternehmen belegen dies. Der Mensch ist das schwächste Element im Sicherheitssystem und bedarf besonderer Aufmerksamkeit.

Wünschenswert ist seine aktive, bewusste und vor allem überzeugte Mitwirkung in der Informationssicherheit.

Um diese zu erreichen, werden in den Unternehmen Security-Awareness-Kampagnen durchgeführt. Die Ziele dieser Kampagnen sind, den Anwendern die Bedeutung eines sicherheitsrelevanten Verhaltens näher zu bringen und sie mit dem notwendigen Wissen sowie den notwendigen Verhaltensregeln auszustatten. Die Grundannahme ist, dass dann automatisch das richtige Verhalten folgen wird. Erfahrungen zeigen jedoch, dass die Existenz von Wissen und Bewusstsein häufig nicht ausreicht, um ein gewünschtes Verhalten zu bewirken bzw. dass Einstellung und Verhalten oft auseinanderklaffen. In dieser Arbeit wird davon ausgegangen, dass weitere Faktoren existieren, die Einstellung und Verhalten beeinflussen. Das Verständnis dieser Faktoren kann dabei helfen, Instrumente, Maßnahmen und Rahmenbedingungen so auszugestalten bzw. zu verbessern, dass ein gewünschtes Verhalten bewirkt wird.

Entsprechend befasst sich diese Arbeit mit der Analyse von ursächlichen Faktoren, die Einstellung und Verhalten der Mitarbeiter in der Informationssicherheit beeinflussen. Dazu wurden zunächst basierend auf Erkenntnissen aus der Literatur potentielle Einflussfaktoren herausgearbeitet. Aufbauend darauf wurde ein Fragebogen entwickelt und eine Befragung in unterschiedlichen Organisationen durchgeführt. Schließlich wurden mittels Korrelations- und Regressionsanalysen die Einflüsse der ausgearbeiteten Faktoren untersucht und interpretiert. Ein besonderer Fokus lag dabei auf der Analyse der Wirkung von Awareness-Kampagnen auf diese Faktoren.

2 Verwandte Arbeiten

Auch wenn das Erscheinen von Beiträgen zur Rolle der Mitarbeiter in der Informationssicherheit in den Beginn der 1990er Jahre zurückgeht, findet sich der Großteil der Literatur ab dem Jahre 2000. Während die Arbeiten zu Beginn eher konzeptioneller bzw. theoretischer Natur waren, wurden zunehmend empirische Studien veröffentlicht.

Ein großer Teil der Arbeiten befasst sich mit Maßnahmen und Instrumenten, mittels derer bei den Mitarbeitern ein sicherheitskonformes Verhalten bewirkt werden kann. Das Spektrum reicht dabei von Sanktionen über Kontrollen bis hin zu Anreizen, sowohl nicht-monetärer als auch monetärer Natur. Einen guten Überblick hierzu geben [BCB10].

Zu Beginn lag der Fokus eher auf Sanktionen, denen ein entsprechender Abschreckungseffekt zugeschrieben wurde [BCB10], [SN90]. Zunehmend wurde aber auch die Bedeutung von Kontrollmaßnahmen festgestellt unter der Annahme, dass allein das Wissen darüber das Verhalten der Mitarbeiter beeinflusst [Wi06]. Insbesondere von der organisationsorientierten Literatur angeregt werden daneben auch Anreize als Maßnahmen diskutiert. Dabei werden sowohl die Verstärkung der sozialen Bindung der Mitarbeiter als motivationserhöhender Faktor [LL02], [LLY03] als auch Belohnungen in nicht-monetärer (z.B. Lob oder Beförderung) und monetärer Form vorgeschlagen und untersucht [BCB10], [KB07], [PSM07].

Neuere empirische Studien untersuchen die Wirkungen dieser Instrumente auf die Einstellung und das Verhalten im Hinblick auf die Informationssicherheit. Ausgehend von der Erkenntnis, dass Einstellung und Verhalten oft nicht übereinstimmen, ist häufig auch die Analyse der Ursachen dieser Diskrepanz der Gegenstand. Die Mehrzahl der Studien basiert auf Befragungen. Da das zukünftige Verhalten nicht direkt erfragbar ist, wird stattdessen die Verhaltensabsicht als dessen Stellvertreter verwendet. In den Studien werden die Einflüsse auf Einstellung und Verhaltensabsicht entweder direkt über die Instrumente und Maßnahmen oder indirekt über aus ihnen abgeleiteten Größen untersucht. Eine Zusammenfassung und Metaanalyse dieser Studien finden sich in [MG13]. Eine der Erkenntnisse der Autoren ist, dass die Studien teilweise zu unterschiedlichen Beurteilungen einzelner Größen gelangen. So hat beispielsweise die „Stärke der Bestrafung“ bei nicht-sicherheitskonformem Verhalten in zwei Studien zwar einen jeweils signifikanten Effekt auf die Verhaltensabsicht, jedoch in der einen Studie einen positiven und in der anderen Studie einen negativen Effekt.

Generell beinhaltet die Durchführung derartiger Studien einige Problembereiche bzw. Limitationen. So besteht auch bei theoretischer Fundierung eine hohe Wahlfreiheit bei der Bestimmung der Einflussgrößen bzw. wie diese bei den Probanden abgefragt werden. Entsprechend zeigen [DH11] explizit, dass auch bei der gleichen zugrundeliegenden Theorie widersprüchliche Ergebnisse resultieren können.

Eine wichtige Rolle spielt dabei auch, wer befragt wird. So verwenden akademische Studien oft Studierende als Stellvertreter für die eigentlich zu befragenden Personen. Gerade im Zusammenhang mit der Informationssicherheit fehlt diesen aber häufig das Vorstellungsvermögen für die entsprechenden Situationen in der Praxis. Werden hingegen die Mitarbeiter in Unternehmen befragt, so besteht die Gefahr des Vertrauensproblems in die Anonymität der Umfrage. Daraus können dann Verzerrungen im Hinblick auf das Abgeben von vermeintlich erwünschten Antworten entstehen.

Einige Studien konzentrieren sich zudem ausschließlich auf Personen, die bereits an einer Security-Awareness-Kampagne teilgenommen haben und somit über das entsprechende Wissen verfügen [BCB10]. Damit wird jedoch der Personenkreis ausgeschlossen, der aufgrund seines möglichen Nicht-Wissens eine besondere Gefährdung der Informationssicherheit darstellen kann. Interessant ist zudem auch die Analyse der Unterschiede zwischen diesen Personengruppen, z.B. um die Wirksamkeit von Awareness-Kampagnen zu untersuchen.

3 Potentielle Einflussfaktoren auf Einstellung und Verhaltensabsicht

Im Gegensatz zu den Studien, die sich damit befassen, mittels welcher Maßnahmen eine gewünschte Einstellung bzw. eine gewünschte Verhaltensabsicht erreicht werden soll, steht in der vorliegenden Studie die Frage im Vordergrund, welche Faktoren für das Entstehen einer bestimmten Einstellung bzw. einer bestimmten Verhaltensabsicht ursächlich sind. Gegenstand ist die Aufarbeitung und Überprüfung von möglichen Einflussfaktoren, die auf diese beiden Größen in der Informationssicherheit wirken. Neben dem Erkenntnisgewinn kann deren Kenntnis einerseits helfen, die gegenwärtig

eingesetzten bzw. in den Studien aufgeführten Instrumente und Maßnahmen zu überprüfen, und andererseits wertvolle Hinweise für die Entwicklung bzw. Weiterentwicklung von Instrumenten geben.

Von besonderem Interesse ist hierbei auch die Analyse der Bedeutung von Awareness-Kampagnen, die in der Praxis zwar ein wichtiges Instrument sind, gleichzeitig in ihrer Wirksamkeit aber sehr kontrovers diskutiert werden. Unstrittig ist, dass auf Wissen nicht automatisch die gewünschte Einstellung und daraus nicht automatisch das gewünschte Verhalten folgt. Welche Bedeutung aber das erlangte Wissen auf Einstellung und Verhaltensabsicht hat und welche Faktoren hier noch begleitend wirken, kann jedoch wichtig für die Weiterentwicklung ebenso wie für die Einbettung von Awareness-Kampagnen in Unternehmen sein.

Da die grundlegenden Einflussgrößen auf Einstellung und Verhalten in der Informationssicherheit ein noch relativ unerforschtes Gebiet sind, bietet sich bei deren Aufarbeitung ein Blick in die Umweltschutzforschung an. Dieses im Hinblick auf das menschliche Verhalten recht gut erforschte Gebiet kann wertvolle Hinweise geben, da auch hier die Umweltzerstörung häufig nicht eine unmittelbare Bedrohung ist (sondern weit weg stattfindet) und sich ein Umweltbewusstsein als Einstellung oft nicht in einem verantwortlichen Umweltverhalten niederschlägt [FW97].

Eine grundlegende Bedeutung für eine Einstellung bzw. eine Verhaltensabsicht wird dabei auch in der Umweltschutzforschung dem Wissen zugemessen [Ku98]. Wissen dient einerseits als Baustein, um überhaupt eine Einstellung bzw. eine Verhaltensabsicht zu erlangen und kann diese andererseits auf eine objektive und sachliche Ebene bringen. Davon ausgehend ist die Durchführung von Awareness-Kampagnen eine wichtige Maßnahme, da auf diesem Weg Wissen über den Gegenstandsbereich vermittelt wird.

Hypothese 1: Das Wissen über das Thema Informationssicherheit sowie über die Sicherheitspolicy des Unternehmens steht in positivem Zusammenhang zu Einstellung und Verhaltensabsicht. Der Faktor wirkt dabei stärker auf die Einstellung.

Auch in der Umweltschutzforschung ist eine der wesentlichen Erkenntnisse, dass deutliche Diskrepanzen zwischen Wissen, Einstellung und Verhaltensabsicht bestehen [Ku98]. Daraus kann gefolgert werden, dass neben dem Wissen weitere Einflussfaktoren auf diese beiden Größen wirken.

In der Umweltwissenschaft wird als eine Einflussgröße die Wahrnehmung einer Bedrohung betrachtet [FW97]. Aufgrund einer mangelnden direkten Erfahrung mit Umweltveränderungen fühlen sich Menschen häufig nicht persönlich bedroht. Dies kann auch auf die Informationssicherheit übertragen werden, da auch hier ein großer Teil der Mitarbeiter keine direkten Erfahrungen mit Sicherheitsvorfällen hat bzw. Kollegen mit derartigen Erfahrungen kennt.

Hypothese 2: Die wahrgenommene Bedrohung steht in positivem Zusammenhang zu Einstellung und Verhaltensabsicht. Der Faktor wirkt dabei stärker auf die Einstellung.

Den Erkenntnissen der Umweltschutzforschung zufolge fühlen sich Menschen ohne das Gefühl einer Bedrohung auch eher nicht verantwortlich für das Ergreifen von Schutzmaßnahmen [FW97]. Aber auch im Falle einer gefühlten Bedrohung besteht die Möglichkeit, die Verantwortlichkeit an anderer Stelle zu sehen und sich auf diese zu verlassen. Gerade im Bereich der Informationssicherheit herrscht vielerorts in den Unternehmen die Ansicht, dass der IT-Bereich die Verantwortung für den Schutz trägt. Entsprechend kann man sich bei dieser Sichtweise auf die Erledigung der Arbeit konzentrieren und empfindet die aus der Informationssicherheit erwachsenden technischen und organisatorischen Restriktionen sogar eher als Behinderung.

Hypothese 3: Das Empfinden von Verantwortung steht in positivem Zusammenhang zu Einstellung und Verhaltensabsicht. Der Faktor wirkt dabei stärker auf die Einstellung.

Verantwortung zu übernehmen bedeutet im Arbeitsalltag oft, dass man zugunsten eines sicherheitskonformen Verhaltens Zeit und/oder sonstige Ressourcen von der Verfolgung der eigentlichen beruflichen Aufgaben abziehen muss. Wenn dann die Einhaltung eines sicherheitskonformen Verhaltens nicht in die Leistungsbeurteilung der Mitarbeiter eingeht, kann ein solches Verhalten sogar kontraproduktiv im Hinblick auf die Erreichung der persönlichen Arbeitsziele wirken. Von dieser Argumentation ausgehend, können zwei Faktoren im Hinblick auf ein sicherheitskonformes Verhalten abgeleitet werden. Ein erster Faktor ist der Zeitdruck, unter dem die Tätigkeiten verrichtet werden. Es kann angenommen werden, dass unter Zeitdruck die Erledigung der Arbeit tendenziell eine größere Rolle spielt als das Einhalten von Sicherheitsvorschriften [GR13]. Zum anderen dürfte hier aber auch der Aufwand, der mit einem sicherheitskonformen Verhalten verbunden ist, eine Rolle für die Mitarbeiter spielen. Je geringer dieser Aufwand ist, desto geringer ist auch das Konfliktpotential zwischen Zielerreichung und Sicherheitskonformität [Ro10]. Dieser aufwandsbezogene Faktor soll im Folgenden als Bequemlichkeit der Informationssicherheit bezeichnet werden.

Hypothese 4: Der Zeitdruck am Arbeitsplatz steht in negativem Zusammenhang zu Einstellung und Verhaltensabsicht. Der Faktor wirkt dabei stärker auf die Verhaltensabsicht.

Hypothese 5: Die Bequemlichkeit im Umgang mit der Informationssicherheit steht in positivem Zusammenhang zu Einstellung und Verhaltensabsicht. Der Faktor wirkt dabei stärker auf die Verhaltensabsicht.

Als weiterer Faktor wird hier die Einschätzung der Wirksamkeit der Informationssicherheitsmaßnahmen durch die Mitarbeiter betrachtet [La08]. Es wird davon ausgegangen, dass die Neigung, Aufwand für ein sicherheitskonformes Verhalten zu betreiben, umso geringer ist, je geringer man die Wirksamkeit der Maßnahmen zur Informationssicherheit im Unternehmen einschätzt. Die hier gemeinte Wirksamkeit umfasst dabei nicht nur die Sicherheitsvorschriften an sich, sondern auch die Art, wie deren Einhaltung im Unternehmen umgesetzt und kontrolliert wird. Ein laxer Umgang hinsichtlich deren Einhaltung kann hier beispielsweise die Zweifel an der Wirksamkeit nähren.

Hypothese 6: Die Einschätzung der Wirksamkeit steht in positivem Zusammenhang zu Einstellung und Verhaltensabsicht. Der Faktor wirkt dabei stärker auf die Verhaltensabsicht.

In einer Studie über Datenverlustrisiken wurde für die USA festgestellt, dass die Neigung zum Datendiebstahl eng mit der empfundenen Integrität und Fairness des Arbeitgebers zusammenhängt [Po09]. Demzufolge kann angenommen werden, dass die empfundene Einstellung des Unternehmens zum Mitarbeiter, im Folgenden als Gerechtigkeit bezeichnet, einen weiteren Faktor darstellt. Eine empfundene hohe Gerechtigkeit würde folglich eher zu einer erhöhten Neigung zur Einhaltung von Sicherheitsvorschriften führen, was konform zu den Erkenntnissen von [LL02] ist.

Hypothese 7: Das Empfinden von Gerechtigkeit seitens des Arbeitgebers steht in positivem Zusammenhang zu Einstellung und Verhaltensabsicht. Der Faktor wirkt dabei stärker auf die Verhaltensabsicht.

In diesem Abschnitt wurden sieben Faktoren identifiziert, die einen Einfluss auf die Einstellung und die Verhaltensabsicht von Mitarbeitern im Hinblick auf die Informationssicherheit haben können. Es sei an dieser Stelle explizit darauf hingewiesen, dass kein Anspruch auf Vollständigkeit erhoben wird. Die Überprüfung dieser Faktoren kann jedoch einen wichtigen Schritt für die weitere Erforschung der Rolle der Mitarbeiter in der Informationssicherheit darstellen. Entsprechend soll im Folgenden in einer empirischen Untersuchung analysiert werden, welchen Einfluss diese Faktoren auf die Einstellung und die Verhaltensabsicht haben. Von Interesse ist zudem, ob die oben genannten Einflussfaktoren bei Teilnehmern an einer Awareness-Kampagne anders wirken als bei Nicht-Teilnehmern.

4 Empirische Untersuchung

4.1 Datenerhebung und Untersuchungsmethodik

Die in die Analyse eingehenden Daten wurden mittels eines Fragebogens erhoben. Als Teilnehmer für die Befragung konnten fünf Organisationen von unterschiedlicher Natur (eine Bank, ein Verband, ein Landesamt sowie zwei Unternehmensberatungen mit unterschiedlichem Fokus) gewonnen werden. Unterstützt durch die Informationssicherheits- oder Datenschutzverantwortlichen wurden die Mitarbeiter der gesamten bzw. von Teilen der Organisation über die Studie in Kenntnis gesetzt und um Teilnahme gebeten. Der Teilnahme war freiwillig und erfolgte anonym. Es ergaben sich insgesamt 277 Fragebögen, die verwertbar waren.

Der Fragebogen bestand aus 25 Fragen, die sich hauptsächlich auf die Einstellung, die Verhaltensabsicht und auf die in Abschnitt 3 aufgearbeiteten Faktoren bezogen. Darüber hinaus wurden Fragen hinsichtlich der Teilnahme an Awareness-Kampagnen und deren Beurteilung gestellt sowie einige Kontrollfragen. Die Entwicklung des Fragebogens vollzog sich über drei Testrunden, bei denen Studierende aus den berufsbegleitenden

akademischen Programmen genutzt wurden, um sicherzustellen, dass die Teilnehmer ein entsprechendes Vorstellungsvermögen für die Fragen aufweisen. Ziel dieser Testrunden war die Prüfung von Sinnhaftigkeit, Relevanz und Verständlichkeit der Fragestellungen. Entsprechend wurden die Fragen modifiziert, ausgetauscht und erweitert, bis schließlich die finale Version entstand.

Die Mehrzahl der Fragen beinhaltet Antwortmöglichkeiten auf einer 4-stufigen Likert-Skala. Daneben wurden auch noch dichotome Fragen verwendet, wenn mehr Antworten keinen Sinn machten, z.B. bei der Frage nach der Teilnahme an einer Awareness-Kampagne.

Variable	Fragen
Einstellung	Wie bedeutsam ist für Sie persönlich das Thema „Informationssicherheit“ im beruflichen Bereich? Für wie wichtig erachten Sie das Thema „Informationssicherheit“ bei Ihrer persönlichen Arbeit?
Verhaltensabsicht	Beabsichtigen Sie, die Regeln und Richtlinien zur Informationssicherheit in Zukunft einzuhalten? Beabsichtigen Sie, in Zukunft die Computer- und Mobiltechnologie-Ressourcen unter Beachtung aller Sicherheitsaspekte einzusetzen? Wofür würden Sie sich entscheiden, wenn Sie zwischen der fristgerechten Erledigung Ihrer Arbeit und der Einhaltung der Informationssicherheitsvorschriften wählen müssten?
Wissen	Wie schätzen Sie Ihren Wissensstand über das Thema „Informationssicherheit“ ein? Wie gut kennen Sie die Maßnahmen, Regeln und Richtlinien hinsichtlich der Informationssicherheit in Ihrer Organisation?
Bedrohung	Für wie bedroht halten Sie Ihre Organisation? Für wie wahrscheinlich schätzen Sie, dass Sie selbst das Angriffsziel sind?
Verantwortung	Wie schätzen Sie Ihre Verantwortlichkeit für die Informationssicherheit in Ihrer Organisation ein?
Bequemlichkeit	Wie empfinden Sie die Maßnahmen zur Informationssicherheit in Ihrer Organisation in Bezug auf Ihre eigene Tätigkeit? Wie bewerten Sie die Praktikabilität der Regeln und Richtlinien hinsichtlich der Informationssicherheit in Ihrer Organisation?
Wirksamkeit	Wie beurteilen Sie Angemessenheit der Maßnahmen zur Informationssicherheit in Ihrer Organisation? Wie beurteilen Sie die Wirksamkeit der Maßnahmen zur Informationssicherheit in Ihrer Organisation? Wie bewerten Sie den Nutzen der Regeln und Richtlinien hinsichtlich der Informationssicherheit in Ihrer Organisation?
Zeitdruck	Verfügen Sie über ausreichend Zeit für die Erledigung Ihrer Tätigkeiten?
Gerechtigkeit	Sind Sie der Meinung, dass Ihre Organisation einen fairen Umgang mit ihren Mitarbeitern pflegt?

Tabelle 1: Zusammensetzung der Einflussgrößen

Mit Ausnahme der Verantwortung, des Zeitdrucks und der Gerechtigkeit wurden jeweils mehrere Fragen für die Kalkulation der in der Untersuchung verwendeten Variablen verwendet. Der Grund dafür war, dass die mitunter vielschichtige Aussage der einzelnen Größen durch weitestgehend einfache Fragen erfragt werden sollten, um den Teilneh-

mern möglichst keinen Interpretationsspielraum zu lassen. Demzufolge wurden die Größen aus unterschiedlichen Perspektiven abgefragt, die Antworten der Fragen danach mittels Z-Transformation auf ein einheitliches Skalenniveau transformiert und schließlich per Mittelwertbildung pro Variable aggregiert. Um sicherzustellen, dass die Antworten auch tatsächlich in die gleiche Richtung zielen, wurde vor der Aggregation jeweils mittels einer exploratorischen Faktorenanalyse analysiert, ob die Items auf einen gemeinsamen Faktor laden und damit ein eindimensionales Konstrukt abbilden. Tabelle 1 enthält die Variablen sowie die diese definierenden Fragen (zum Teil aus Darstellungsgründen in modifizierter Form).

Mit den so gewonnenen Variablen wurden Korrelations- und Regressionsanalysen durchgeführt, um die Zusammenhänge und Abhängigkeiten zu bewerten. Basierend auf Signifikanztests wurden schließlich die Ergebnisse interpretiert. Die Berechnungen wurden mit der Statistiksoftware SPSS durchgeführt.

In einem ersten Schritt wurde dabei analysiert, welchen Einfluss die sieben herausgearbeiteten Faktoren (im Folgenden auch als „unabhängige Variablen“ bezeichnet) auf Einstellung und Verhaltensabsicht („abhängige Variablen“) unter Verwendung aller Befragten haben. Dazu wurde zunächst über eine Korrelationsanalyse die Stärke der bivariaten Zusammenhänge zwischen den Variablen untersucht. Im Anschluss daran wurden über Regressionsanalysen die multivariaten Beziehungen der sieben Faktoren auf die beiden abhängigen Variablen analysiert. In Erweiterung zur Korrelationsanalyse können bei der Regressionsanalyse Zusammenhänge unter simultaner Verwendung mehrerer unabhängiger Einflussfaktoren untersucht werden. Die Analysen wurden in einem zweiten Schritt für die Gruppe der Befragten, die bereits an einer Awareness-Kampagne teilgenommen haben, und die Gruppen, bei denen das nicht der Fall war, wiederholt, um auf Basis der Unterschiede die Wirkungsweise und Wirksamkeit von Awareness-Kampagnen zu untersuchen.

4.2 Ergebnisse und Interpretation

Im Folgenden werden die Ergebnisse der empirischen Analyse in der Reihenfolge „alle Befragten“, „Teilnehmer von Awareness-Kampagnen“ und „Nicht-Teilnehmer von Awareness-Kampagnen“ dargestellt. Tabelle 2 enthält das Ergebnis der Korrelationsanalyse für alle Befragten. Die in der Tabelle aufgeführten Werte drücken die Stärke der bivariaten Zusammenhänge aus. Die stellenweise an den Korrelationswerten anhängenden Sterne geben das Signifikanzniveau des jeweiligen Wertes an. Signifikanz heißt hier, dass mit einer Wahrscheinlichkeit von mindestens 99% (**) bzw. mindestens 95% (*) tatsächlich ein Zusammenhang auf Populationsebene besteht und damit der Wert nicht rein zufällig ist. Die Nummern in der Kopfzeile der Tabelle korrespondieren mit den Nummern der Variablen in den Zeilen. Es sind vor allem die mit 1 und 2 überschriebenen Spalten von Interesse, da sie die Korrelationen von Einstellung bzw. Verhaltensabsicht und den restlichen Variablen ausdrücken.

Mit einem Wert von 0,451 besteht eine mittelstarke Korrelation zwischen der Einstellung und der Verhaltensabsicht. Die Verhaltensabsicht ist somit kein reines Resultat der Einstellung, sondern wird von weiteren Faktoren beeinflusst. Betrachtet man die Korre-

lationen zwischen der Einstellung und den sieben möglichen Einflussfaktoren (Spalte 1), so zeigen die Werte einen hoch signifikanten Zusammenhang zu Wissen, Verantwortung und Wirksamkeit. Die eindeutig stärksten Zusammenhänge bestehen dabei zu Wissen und Verantwortung, die somit den größten Einfluss auf die Einstellung haben.

Variable	1	2	3	4	5	6	7	8	9
Abhängig:									
1. Einstellung	—								
2. Verhaltensabsicht	,451**	—							
Unabhängig:									
3. Wissen	,461**	,319**	—						
4. Bedrohung	-,061	,001	-,053	—					
5. Verantwortung	,385**	,191**	,280**	-,033	—				
6. Zeitdruck	-,031	-,170**	,053	-,049	-,054	—			
7. Bequemlichkeit	,142*	,253**	,086	,009	,078	-,226**	—		
8. Wirksamkeit	,160**	,228**	,059	-,056	-,006	-,208**	,434**	—	
9. Gerechtigkeit	,122*	,149*	,140*	-,036	,120*	,228**	,126*	,200**	—

Anmerkungen: N = 277, **p ≤ ,01, *p ≤ ,05

Tabelle 2: Ergebnis der Korrelationsanalyse (Basis: alle Befragten)

Verglichen damit zeigen die Korrelationen zwischen der Verhaltensabsicht und den Einflussgrößen ein anderes Bild. Hier sind zwar auch die Zusammenhänge mit Wissen und Verantwortung hochsignifikant, jedoch in deutlich geringerer Stärke. Dafür kommen hier zusätzlich den Variablen Bequemlichkeit, Wirksamkeit und Zeitdruck eine wichtige Bedeutung zu, was die Unterschiede zwischen der Einstellung und der Verhaltensabsicht zumindest teilweise erklären kann. Zu beiden besteht noch ein schwacher, aber signifikanter Zusammenhang mit der Gerechtigkeit, wogegen die Zusammenhänge mit der empfundenen Bedrohung weder in den Werten noch in den Signifikanzniveaus von Null verschieden sind und somit keine Rolle spielen dürften.

	Einstellung					Verhaltensabsicht				
Variable	b	SD	ß	t	p	b	SD	ß	t	p
(Konstante)	,019	,041		,464	,643	,000	,038		-,004	,997
Wissen	,328	,050	,358	6,575**	,000	,199	,047	,252	4,224**	,000
Bedrohung	,000	,050	,000	-,010	,992	,029	,048	,035	,617	,538
Verantwortung	,238	,043	,303	5,568**	,000	,074	,040	,110	1,844	,066
Zeitdruck	-,001	,043	-,002	-,029	,977	-,070	,041	-,104	-1,728	,085
Bequemlichkeit	,028	,067	,025	,420	,675	,125	,064	,127	1,976*	,049
Wirksamkeit	,174	,077	,133	2,250	,250	,151	,073	,133	2,064*	,040
Gerechtigkeit	,015	,043	,019	,348	,728	,025	,040	,037	,623	,534
	R^2 = ,317; F = 17,024**					R^2 = ,183; F = 8,250**				

Tabelle 3: Ergebnis der Regressionsanalysen (Basis: alle Befragten)

Für eine multivariate Analyse der Beziehungen wurde sowohl für die Einstellung als auch für die Verhaltensabsicht eine Regressionsanalyse mit den sieben Einflussfaktoren als unabhängige Variablen berechnet. Die Ergebnisse sind in Tabelle 3 dargestellt. Während das R^2 den Anteil der erklärten Varianz angibt, drückt der F-Wert bzw. dessen

Signifikanzniveau aus, ob die in der Stichprobe gefundenen Zusammenhänge auf die Population übertragbar sind.

Für jede der Regressionsanalysen werden in Tabelle 3 zunächst mit b die unstandardisierten Koeffizienten der Regressionsgleichung und mit SD deren Standardfehler angegeben. Um den Erklärungsgehalt der unabhängigen Variablen miteinander zu vergleichen, eignen sich die b jedoch nicht, da den Variablen unterschiedliche Antwortskalen zugrunde lagen. Hierzu werden die standardisierten Beta-Koeffizienten verwendet, die in der Spalte ß ausgewiesen sind. Die Spalten t und p drücken das Signifikanzniveau der Regressionskoeffizienten über deren t- und die zugehörigen p-Werte aus. Signifikanz bedeutet hier, dass der jeweilige Koeffizient bedeutsam und von Null verschieden ist und innerhalb einer bestimmten Bandbreite um den ausgewiesenen Wert auch für die Populationsebene angenommen wird. Je geringer der p-Wert, desto größer ist die Sicherheitswahrscheinlichkeit für den jeweiligen Koeffizienten und desto geringer ist dessen Bandbreite (Konfidenzintervall).

Die Regressionsanalyse von Einstellung auf alle unabhängigen Variablen bestätigt im Wesentlichen die Ergebnisse der Korrelationsanalyse. Sowohl die ß als auch die Signifikanzniveaus weisen hier das Wissen wie auch die Verantwortung als die wichtigsten Einflussfaktoren aus. Die Wirksamkeit hat in dieser Totalbetrachtung zwar noch ein vergleichsweises hohes ß, jedoch ist dieses nicht mehr signifikant, weshalb deren Einfluss nicht als gesichert angesehen werden kann. Auch bei der Regressionsanalyse von Verhaltensabsicht auf die Faktoren bestätigen sich die Ergebnisse aus der Korrelationsanalyse. Zwar hat auch hier das Wissen den bedeutendsten Einfluss, jedoch spielen daneben die Bequemlichkeit und die Einschätzung der Wirksamkeit der Informationssicherheit eine wesentliche Rolle. Es folgen Verantwortung und Zeitdruck, deren Signifikanz jedoch nur noch marginal ist. In beiden Regressionsanalysen haben weder die Gerechtigkeit noch die Bedrohung einen signifikanten Einfluss.

Zusammenfassend kann man aus den bisherigen Analysen schlussfolgern, dass die Vermittlung von Wissen und das Erzeugen eines Verantwortungsgefühls hinsichtlich der Informationssicherheit bei den Mitarbeitern eine wesentliche Rolle spielen, um eine gewünschte Einstellung zu bewirken. Diese führt jedoch eindeutig nicht automatisch zu dem gewünschten Verhalten. So sind Wissen und Verantwortungsgefühl zwar auch hier relevante Einflussgrößen, jedoch wird die Verhaltensabsicht noch zusätzlich von den Faktoren Bequemlichkeit, Wirksamkeit und Zeitdruck determiniert. Um ein gewünschtes Verhalten zu erzeugen, müssen die Mitarbeiter also zusätzlich zur Einstellung noch von der Wirksamkeit der Informationssicherheitsmaßnahmen überzeugt sein, wobei diese die Mitarbeiter so wenig wie möglich an der Ausübung ihrer Tätigkeiten behindern dürfen (Bequemlichkeit). Zusätzlich sollten sie keinem hohen Zeitdruck ausgesetzt sein, so dass Zeit für die Beachtung und Befolgung der Sicherheitsmaßnahmen vorhanden ist. Mit Ausnahme der (empfundenen) Bedrohung wurden die oben aufgestellten Hypothesen bivariat mittels der Korrelationsanalyse bestätigt, multivariat setzten sich in den Regressionsanalysen die jeweils wichtigsten Einflussfaktoren durch. Diesen kommt somit in der Totalbetrachtung eine ausschlaggebende Bedeutung zu.

Variable	1	2	3	4	5	6	7	8	9
Abhängig:									
1. Einstellung	—								
2. Verhaltensabsicht	,445**	—							
Unabhängig:									
3. Wissen	,493**	,343**	—						
4. Bedrohung	-,081	,022	-,053	—					
5. Verantwortung	,419**	,260**	,287**	,000	—				
6. Zeitdruck	-,080	-,199**	,082	-,026	,022	—			
7. Bequemlichkeit	,106	,191**	-,003	,035	,071	-,227**	—		
8. Wirksamkeit	,165*	,215**	,050	-,019	-,021	-,229**	,428**	—	
9. Gerechtigkeit	,162*	,191**	,171*	-,058	,160*	,217**	,137*	,226**	—

Anmerkungen: n = 219, **p ≤ ,01, *p ≤ ,05

Tabelle 4: Ergebnis der Korrelationsanalyse (Basis: mit Awareness-Kampagne)

Von Interesse war nun zu untersuchen, ob die Teilnahme bzw. Nicht- Teilnahme an einer Awareness-Kampagne zu einem anderen Bild im Hinblick auf die gefundenen Zusammenhänge führt. Die Ergebnisse für die Befragten, die bereits an einer Kampagne teilgenommen haben, sind in den Tabellen 4 und 5 dargestellt. Es zeigt sich ein ähnliches Bild, jedoch sind Wissen und Verantwortung ausgeprägter in ihrer Einflussstärke auf Einstellung und Verhaltensabsicht. Dafür sind die Zusammenhänge von Bequemlichkeit und Wirksamkeit mit der Verhaltensabsicht schwächer, wie die Korrelationen zeigen.

	Einstellung					Verhaltensabsicht				
Variable	b	SD	ß	t	p	b	SD	ß	t	p
(Konstante)	-,036	,043		-,843	,400	-,035	,043		-,815	,416
Wissen	,362	,054	,395	6,697**	,000	,242	,055	,289	4,425**	,000
Bedrohung	-,050	,051	-,054	-,974	,331	,032	,051	,038	,620	,536
Verantwortung	,254	,046	,323	5,476**	,000	,120	,047	,168	2,575*	,011
Zeitdruck	-,070	,046	-,090	-1,518	,130	-,119	,046	-,168	-2,572*	,011
Bequemlichkeit	,035	,072	,031	,486	,628	,092	,072	,089	1,274	,204
Wirksamkeit	,147	,080	,117	1,829	,069	,134	,081	,117	1,647	,101
Gerechtigkeit	,001	,044	,002	,028	,978	,028	,044	,041	,629	,530
	R^2 = ,368; F = 17,031**					R^2 = ,224; F = 8,475**				

Tabelle 5: Ergebnis der Regressionsanalysen (Basis: mit Awareness-Kampagne)

In der Regressionsanalyse sind beide Koeffizienten ebenfalls schwächer und zudem nicht mehr signifikant. Eine mögliche Interpretation ist, dass das im Rahmen der Awareness-Kampagnen vermittelte Verständnis hierzu einen Beitrag leistet. So entsteht möglicherweise die Erkenntnis, dass mit der Informationssicherheit gewisse Unbequemlichkeiten einhergehen, die nun aber in ihrer Notwendigkeit besser verstanden und somit auch eher akzeptiert werden. Auch die Wirksamkeit kann mit einem umfangreicheren Wissen besser eingeschätzt werden. Als Einflussfaktor auf die Verhaltensabsicht ist hier der Zeitdruck noch signifikant und hat eine gleich hohe Einflussstärke wie die Verantwortung. Eine mögliche Interpretation ist, dass man trotz besseren Wissens tendenziell umso weniger geneigt ist, die Sicherheitsvorschriften einzuhalten, je weniger Zeit zur Verfügung steht. Nach der Korrelationsanalyse spielt hier auch noch die Gerechtigkeit

eine Rolle, was jedoch in der Regressionsanalyse nicht bestätigt wird. Von der Bedrohung geht wiederum kein statistisch relevanter Einfluss aus.

Variable	1	2	3	4	5	6	7	8	9
Abhängig:									
1. Einstellung	—								
2. Verhaltensabsicht	,451**	—							
Unabhängig:									
3. Wissen	,332*	,207	—						
4. Bedrohung	,091	-,031	,067	—					
5. Verantwortung	,366**	-,004	,272*	-,183	—				
6. Zeitdruck	,105	-,064	-,038	-,152	-,288*	—			
7. Bequemlichkeit	,110	,485**	,308*	-,041	,109	-,239	—		
8. Wirksamkeit	,224	,379**	,089	-,230	-,009	-,124	,500**	—	
9. Gerechtigkeit	-,072	-,085	,068	,053	-,002	,302*	,102	,171	—

Anmerkungen: n = 54, **p ≤ ,01, *p ≤ ,05

Tabelle 6: Ergebnis der Korrelationsanalyse (Basis: ohne Awareness-Kampagne)

Für die Gruppe der Befragten, die nicht an einer Awareness-Kampagne teilgenommen haben, ergibt sich ein deutlich unterschiedliches Bild. Die Ergebnisse sind in den Tabellen 6 und 7 dargestellt. Bei der Einstellung fällt zunächst auf, dass der Zusammenhang mit dem Wissen nicht mehr die Stärke und das Signifikanzniveau hat wie in den Analysen zuvor, d.h. das Wissen hat bei diesen Befragten einen geringeren Einfluss auf die Beurteilung der Wichtigkeit der Informationssicherheit als bei den anderen. Stattdessen spielt hier vor allem die Verantwortung eine signifikante Rolle.

	Einstellung					Verhaltensabsicht				
Variable	b	SD	ß	t	p	b	SD	ß	t	p
(Konstante)	,321	,111		2,907	,006	,130	,092		1,409	,166
Wissen	,252	,114	,278	2,199*	,033	,079	,095	,118	,826	,414
Bedrohung	,415	,151	,343	2,747**	,009	,025	,126	,028	,198	,844
Verantwortung	,346	,096	,467	3,610**	,001	-,033	,080	-,060	-,414	,681
Zeitdruck	,231	,102	,302	2,260*	,029	,010	,085	,018	,121	,904
Bequemlichkeit	-,135	,165	-,118	-,821	,416	,305	,137	,359	2,219*	,032
Wirksamkeit	,703	,215	,457	3,271**	,002	,252	,179	,222	1,409	,166
Gerechtigkeit	-,046	,117	-,048	-,394	,695	-,105	,097	-,148	-1,079	,287
	R^2 = ,443; F = 4,889**					R^2 = ,291; F = 2,527**				

Tabelle 7: Ergebnis der Regressionsanalysen (Basis: ohne Awareness-Kampagne)

In der Regressionsanalyse hat zudem der Faktor Wirksamkeit eine fast gleich hohe Bedeutung. Im Gegensatz zu allen zuvor gemachten Analysen sind hier erstmals die empfundene Bedrohung sowie, mit einem positiven Wert, der Zeitdruck signifikante Einflussfaktoren mit einem relativ hohen Bedeutungsgewicht. Eine mögliche Interpretation ist, dass Befragte mit hohem Zeitdruck am Arbeitsplatz die Bedeutung der Informationssicherheit tendenziell umso höher einschätzen, je bedrohter sie sich fühlen, da ihnen kaum Zeit zur Verfügung steht, um angemessen darauf zu reagieren. Hinzu kommt noch das Verantwortungsgefühl. Bei der Verhaltensabsicht sind signifikante bivariate Zusammenhänge nur noch bei der Bequemlichkeit und der Wirksamkeit vorhanden, jedoch

mit vergleichsweise hoher Stärke. In der Regressionsanalyse verbleibt die Bequemlichkeit als einziger signifikanter Faktor. Die Bedeutung dieser beiden Größen für die Verhaltensabsicht könnte ein Hinweis darauf sein, dass das Fehlen entsprechenden Wissens über die unternehmensspezifische Informationssicherheitsarchitektur zu einer eigennützigen Betrachtung und Bewertung derselben führt. Wird sie als hinderlich empfunden, so wird man die Sicherheitsvorschriften tendenziell eher nicht befolgen. Aufgrund des fehlenden objektiven Beurteilungsvermögens werden diese dann auch eher als unwirksam betrachtet, um das Verhalten zu rechtfertigen. Auch hier spielt die Gerechtigkeit weder für die Einstellung noch für die Verhaltensabsicht eine Rolle.

Zusammenfassend haben die differenzierten Analysen einige zusätzliche Einsichten gebracht. So haben bei den Teilnehmern an einer Awareness-Kampagne das Wissen wie auch die Verantwortung einen wesentlich bedeutsameren Einfluss auf die Einstellung hinsichtlich der Notwendigkeit und Wichtigkeit der Informationssicherheit als bei der anderen Gruppe. Bei der Verhaltensabsicht wird der Unterschied zwischen beiden Gruppen noch deutlicher. Während bei den Teilnehmern Wissen und Verantwortung ergänzt um Zeitdruck die maßgeblichen Einflussfaktoren darstellen, sind es bei der anderen Gruppe die Bequemlichkeit und Wirksamkeit. Aus Sicht der Informationssicherheit ist es somit zweckmäßig, Wissen und Fähigkeiten zu vermitteln, um ein entsprechendes Verständnis für die Sicherheitsmaßnahmen zu erreichen, wozu die Awareness-Kampagnen grundsätzlich ein geeignetes Instrument sind.

	alle Befragten		mit Awareness-K.		ohne Awareness-K.	
	Einst.	V.absicht	Einst.	V.absicht	Einst.	V.absicht
Hypothese 1 (Wissen)	++	++	++	++	++	o
Hypothese 2 (Bedrohung)	o	o	o	o	+	o
Hypothese 3 (Verantwortung)	++	+	++	++	++	o
Hypothese 4 (Zeitdruck)	o	+	o	+	-	-
Hypothese 5 (Bequemlichkeit)	+	++	o	+	o	++
Hypothese 6 (Wirksamkeit)	+	++	+	+	+	+
Hypothese 7 (Gerechtigkeit)	+	+	+	+	o	o

++ Korrelations- und Regressionsanalyse signifikant zustimmend

\+ Korrelations- oder Regressionsanalyse signifikant zustimmend

o kein signifikanter Zusammenhang

\- Korrelations- oder Regressionsanalyse signifikant ablehnend

Tabelle 8: Zusammenfassung der Ergebnisse

Insgesamt hat die Untersuchung zum Ergebnis, dass zwar alle der herausgearbeiteten Faktoren mit Einstellung und Verhaltensabsicht in Zusammenhang stehen bzw. darauf einen Einfluss haben, jedoch in unterschiedlicher Stärke (vgl. auch Tabelle 8). So haben vor allem Wissen und Verantwortung den maßgeblichen Einfluss auf die Einstellung, während im Vergleich dazu bei der Verhaltensabsicht noch Bequemlichkeit, Wirksamkeit und Zeitdruck eine wichtige Rolle spielen. Abgesehen von einer Ausnahme hat die Bedrohung sich für Einstellung und Verhaltensabsicht als irrelevant erwiesen. Auch der Faktor Gerechtigkeit spielt nur eine untergeordnete Rolle.

5 Fazit

Die Untersuchung hat gezeigt, dass das Vorhandensein von Wissen über sowie das Verantwortungsgefühl für die Informationssicherheit einen maßgeblichen Einfluss auf das Vorhandensein einer positiven Einstellung der Mitarbeiter hat. Damit sich dies aber auch in der entsprechenden Verhaltensabsicht niederschlägt, müssen zusätzlich die Rahmenbedingungen für die Mitarbeiter stimmen. So muss der Umgang mit der Informationssicherheit möglichst bequem für die Mitarbeiter sein, im Sinne dass sie sie möglichst nicht in der Verfolgung ihrer eigentlichen Leistungsziele behindert. Zudem sollten die Mitarbeiter von der Wirksamkeit der Maßnahmen zur Informationssicherheit überzeugt sein, was einerseits eine entsprechende Aufklärung bedingt, andererseits aber auch mit deren Gestaltung zusammenhängt. Auch die notwendige Zeit für die Befolgung der Maßnahmen sollte gegeben sein. Schließlich spielt auch die empfundene Gerechtigkeit seitens des Arbeitgebers noch eine marginale Rolle. Die Beeinflussung dieser Faktoren liegt aber nicht allein in der Hand der IT-Bereiche im Unternehmen. Insbesondere die Faktoren Zeitdruck und Gerechtigkeit unterliegen eher übergeordneten organisatorischen bzw. unternehmenskulturellen Einflüssen. Für einige der Faktoren spielt die Vermittlung von Wissen, Fähigkeiten und Verständnis eine wichtige Rolle. Die Studie zeigt, dass Awareness-Kampagnen hier ein geeignetes Instrument sein können, auch um das Verständnis der Mitarbeiter auf eine objektivere Basis zu stellen.

Als eine Limitation dieser Studie, die gleichermaßen auch für andere Studien dieser Art gilt, muss an dieser Stelle noch festgestellt werden, dass als verhaltensbezogene Zielvariable die Verhaltensabsicht verwendet wurde. Für die Informationssicherheit relevant ist jedoch letztlich das tatsächliche Verhalten, das nicht zwangsläufig mit der Verhaltensabsicht übereinstimmen muss. Wissenschaftliche Erkenntnisse vor allem aus dem neurobiologischen Bereich deuten darauf hin, dass insbesondere wenn sich Handlungen häufig wiederholen bzw. wenn Zeitdruck besteht, bewusstes Verhalten durch Automatisierungen bzw. tief im Menschen verwurzelte Handlungsheuristiken verdrängt werden [Ro03]. Hierauf setzen beispielsweise auch Angriffstechniken, die dem Social Engineering zugeschrieben werden. Je automatisierter Handlungen am Arbeitsplatz erfolgen, desto größer ist die Gefahr, des Auseinanderklaffens von Verhaltensabsicht und Verhalten. Letzteres kann jedoch nicht abgefragt, sondern müsste mittels Beobachtung gemessen werden. Dazu wären Laborexperimente bzw. Feldstudien notwendig, die die hier gewonnen Ergebnisse validieren könnten. Auch die R^2-Werte in den Regressionsanalysen zeigen, dass mit den untersuchten Faktoren weder Einstellung noch Verhaltensabsicht vollständig erklärt werden können. Somit besteht weiterer Forschungsbedarf, für den diese Studie eine Grundlage bilden kann.

Literaturverzeichnis

[BCB10] Bulgurcu, B.; Cavusoglu, H.; Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. In MIS Quarterly, 34(3), 2010, S. 523-548.

[DH11] D'Arcy, J.; Herath, T.: A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. In European Journal of Information Systems, 20, 2011, S. 642-658.

[FW97] Fuhrer, U.; Wölfing, S.: Von den sozialen Grundlagen des Umweltbewußtseins zum verantwortlichen Umwelthandeln: Die sozialpsychologische Dimension globaler Umweltproblematik, Bern, Göttingen, 1997.

[KB07] Kirsch, L.; Boss, S.: The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines, In ICIS 2007 Proceedings, Paper 103, 2007.

[Ku98] Kuckartz, U.: Umweltbewusstsein und Umweltverhalten. Berlin, 1998.

[MR13] Goeken, M.; Roßbach, P.: Informationssicherheit und Informationssicherheitsmanagement: Grundlagen, Herausforderungen und methodische Unterstützung, In IT-Governance, 7(14), 2013, S. 3-7.

[La08] Lantermann, E.-D.: Umweltbewußtsein und umweltbewußtes Handeln, 2008, http://www.uni-kassel.de/fb4/psychologie/personal/lantermann/umwelt/umweltbewusstsein1.pdf, abgerufen am 18.4.2013.

[LL02] Lee, J.; Lee, Y.: A Holistic Model of Computer Abuse Within Organizations, In Information Management and Computer Security, 10(2), 2002, S. 57-63.

[LLY03] Lee, S. M.; Lee, S. G.; Yoo, S.: An Integrative Model of Computer Abuse based on Social Control and General Deterrence Theories, In Information and Management, 41(6), 2003, S. 707-718.

[MG13] Milicevic, D.; Goeken, M.: Systematic Review and Meta-Analysis of IS Security Policy Compliance Research. First Steps towards Evidence-Based Structuring of the IS Security Domain, In Proceedings der WI2013, 2013, S. 1067-1081.

[Po09] Ponemon: Data Loss Risks During Downsizing, 2009, https://www4.symantec.com/Vrt/offer?a_id=78695, abgerufen am 17.4.2013.

[PSM07] Pahnila, S.; Siponen, M.; Mahmood, A.: Employees' Behavior towards IS Security Policy Compliance, In Proceedings of the 40th Hawaii International Conference on System Sciences, Los Alamitos 2007, S. 156-166.

[Ro10] Roßbach, P.: Der Faktor Mensch in der IT-Sicherheit: data loss prevention, In Die Bank, 12, 2010, S. 58-63.

[Ro03] Roth, G.: Fühlen, Denken, Handeln: Wie das Gehirn unser Verhalten steuert, Frankfurt, 2003.

[SN90] Straub, D. W.; Nance, W. D.: Discovering and Disciplining Computer Abuse in Organizations: A Field Study, In MIS Quarterly, 14(1), 1990, S. 45-60.

[Wi06] Willison, R.: Understanding the Perpetration of Employee Computer Crime in the Organisational Context, In Information and Organization, 16(4), 2006, S. 304-324.