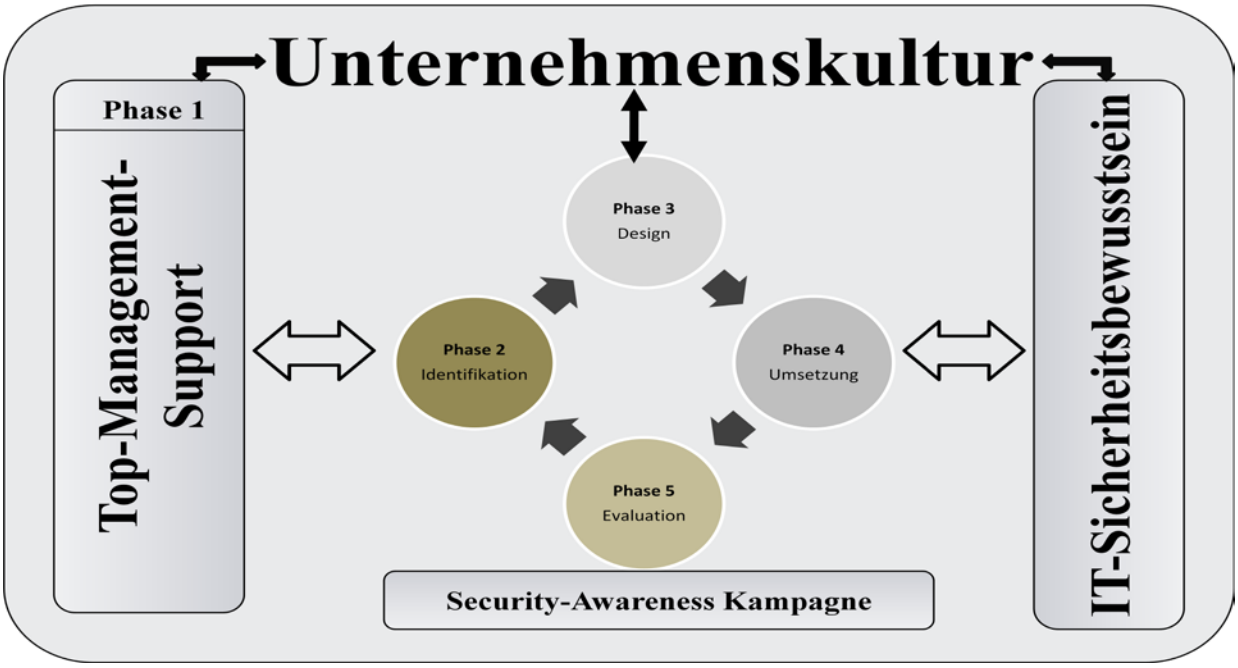
IWI Diskussionsbeiträge
 # 36 (24. Oktober 2009)[1]
ISSN 1612-3646

Stärkung des IT-Sicherheitsbewusstseins unter Berücksichtigung psychologischer und pädagogischer Merkmale

Jörg Uffen [2] und **Michael H. Breitner** [3]



[1] Kopien oder eine PDF-Datei sind auf Anfrage erhältlich: Institut für Wirtschaftsinformatik, Leibniz Universität Hannover, Königsworther Platz 1, 30167 Hannover (www.iwi.uni-hannover.de).

[2] Doktorand, Institut für Wirtschaftsinformatik (uffen@iwi.uni-hannover.de).

[3] Professor für Wirtschaftsinformatik und Betriebswirtschaftslehre und Direktor des Instituts für Wirtschaftsinformatik (breitner@iwi.uni-hannover.de).

Inhaltsverzeichnis

Abstract

Wissen und Informationen sind die Basis der Geschäftsprozesse und können durch den intelligenten Einsatz der Informations- und Kommunikationstechnologie innerhalb einer Organisation zu einer Steigerung der Wettbewerbsfähigkeit führen. Dies macht die Sicherung und den Schutz der Informationssysteme immer wichtiger. Doch trotz der in den letzten Jahren sich abzeichnenden Intensivierung von IT-Sicherheitsmaßnahmen im Hard- und Softwarebereich, stellen Unwissenheit, Fahrlässigkeit und Irrtum des Faktors Mensch in den Organisationen das größte Gefahrenpotenzial dar. Das Risikomanagement fokussiert sich zunehmend auf die Reduktion des „Risikofaktors Mensch“, indem komplexe Security Awareness Konzepte konzipiert werden, in denen eine Sensibilisierung und Motivation für nachhaltiges IT-Sicherheitsverhalten bewirkt werden soll. Pädagogische Ansätze und Menschenbilder, z. B. des „complex man“, über die individuelle Anreizsysteme entwickelt werden, sind die Basis für umfassende Security Awareness Konzepte. Deren Konkretisierung soll nachfolgend diskutiert und analysiert, indem konkrete Handlungsempfehlungen für Unternehmen und Organisationen herausgearbeitet werden sollen.

1 Einführung und Motivation

Im Zuge der letzten Jahrzehnte vollzog sich eine konsequente Wandlung von einer materiell bestimmten Industriegesellschaft zu einer digital vernetzten Informationsgesellschaft. Neben den klassischen Produktionsfaktoren haben sich Wissen und Informationen als entscheidender

Erfolgsfaktor etabliert[4]. Wissen und Informationen sind die Basis der Geschäftsprozesse und können durch den intelligenten Einsatz der Informations- und Kommunikationstechnologie innerhalb einer Organisation zu einer Steigerung der Wettbewerbsfähigkeit führen.

Allerdings macht die zunehmende Integration von Kunden, Lieferanten und Partnern in die Geschäftsprozesse von Unternehmen und der damit stetig wachsenden Zahl der Mediendienste die Sicherung der Informationssysteme immer komplexer und risikobehafteter. Nahezu jedes Unternehmen verfügt über technische Einrichtungen, wie Virenscanner und Firewalls, die bei systematischer Aktualisierung und adäquater Konfiguration den größten Ansturm externer Angriffe durch Trojaner, Würmer und Viren abwehren kann[5]. Doch trotz der Intensivierung von IT-Sicherheitsmaßnahmen im Hard- und Softwarebereich stellen Unwissenheit, Fahrlässigkeit und Irrtum des Faktors Mensch in den Organisationen das größte Gefahrenpotenzial dar[6]. Technische Einrichtungen können nur bekannte, konfigurierte Angriffe abwehren, während ein sensibilisierter Mensch auch potenziell unbekannte Attacken wahrnehmen, mit vorhandenem Wissen abgleichen und entsprechende Gegenmaßnahmen einleiten kann. Dies hat zur Folge, dass sich das IT-Risikomanagement zunehmend auf die Reduktion des „Gefahrenpotenzials Mensch“ fokussieren muss, um über Sensibilisierung das Risiko auf ein akzeptables Maß reduzieren zu können.

Ein wirkungsvolles Instrument stellt die Konzeption einer umfassenden Kampagne dar, um die Generierung von Sicherheitsbewusstsein (neudeutsch: Security-Awareness) bei den verschiedenen Mitarbeitern anzuregen. Das Management der Informationssicherheit steht dabei vor der umfassenden Aufgabe, die verschiedenen Mitarbeitertypen in eine Kampagne zu internalisieren und deren Verhalten über pädagogische Maßnahmen und konkrete Motivationsstrukturen gezielt lenkbar und einschätzbar zu gestalten. In diesem Kontext wird die Interdisziplinarität der Wirtschaftsinformatik bzw. des Managements der Informationssicherheit zu ausgewählten Elementen der Pädagogik, Didaktik, Personalwirtschaftslehre und Organisationspsychologie deutlich. Pädagogisches bzw. didaktisches Handeln strebt dabei gezielte Veränderungen im Wissen, Können und Wollen eines Menschen an[7], während die Organisationspsychologie einen konkreten Einblick in die Rolle, die Eigenschaften und Bedürfnisse, Motive, Erwartungen, sowie das Verhalten und die Einstellungen des Mitarbeiters innerhalb einer Organisation herstellt. Diese Punkte unterstreichen die Notwendigkeit der Heranziehung von in der Organisationstheorie angewandten Menschenbildern, um daraus über gezielt gesetzte Anreize und abgestimmtem Führungsverhalten aus der Personalwirtschaftstheorie normative Handlungsempfehlungen zur konkreten Steuerung von menschlichem Verhalten geben zu können. Primäres Ziel dieses Aufsatzes ist die Konzeption eines langfristigen und vor allem nachhaltigen Security Awareness Konzeptes, welches auf der Grundlage der angesprochenen interdisziplinären Themenfelder erfolgen soll.

[4] vgl. Wirtz/ Sammerl (2003), S. 83
[5] vgl. Fox/ Kaun (2005), S. 329
[6] vgl. <kes>/ Microsoft (2008), S. 18ff.
[7] vgl. Krapp (2006), S. 125

Begonnen werden soll im Abschnitt 2 mit der Darstellung notwendiger Grundlagen der Informationssicherheit. Im Anschluss daran erfolgt – in Abschnitt 3 – eine Analyse des Themas Mensch, mit dessen Lernfähigkeit, Wesens- und Verhaltensmerkmalen sowie den daraus abgeleiteten Motivationsgrundsätzen. Hieraus ergeben sich für das Risikomanagement spezifische Anforderungen, die in eine Security Awareness Kampagne Berücksichtigung finden müssen. Im Abschnitt 4 werden diese Erkenntnisse in ein Security Awareness Konzept integriert und zu konkreten Handlungsempfehlungen zur Unterstützung des Risikomanagements konkretisiert.

2 Stellenwert von Informationssicherheit

Fast ausschließlich werden Informationen heute mit IT-Hilfsmitteln erfasst, aufbereitet, verteilt und archiviert[8]. Informationen, Wissen und Kommunikation beeinflussen nahezu alle Geschäftsprozesse, wodurch ein wichtiger Wettbewerbsfaktor geschaffen wurde. Sicherheitslücken in IT-Systemen, verursacht durch interne oder externe Ereignisse oder durch regelwidrige Handlungsentscheidungen, bergen die Gefahr, dass Unternehmensziele verfehlt werden oder der Fortbestand eines Unternehmens gefährdet wird. Die IT-Ausfallrisiken innerhalb einer Organisation nehmen durch immer komplexere Prozesse, weit verflochtene Unternehmensnetzwerke, den sich verschärfenden Wettbewerb oder wachsende Compliance-Vorgaben stetig zu[9]. Aus diesem Grund ist ein durchgehender und kontrollierter Umgang mit auftretenden Risiken unausweichlich. Generell kann dies nur erfolgen, wenn es zu einer bewussten und kontrollierten Auseinandersetzung mit vorhandenen Risiken kommt. Ziel der IT-Sicherheit ist somit die Gewährleistung, IT-Systeme und die mit ihnen verarbeiteten Informationen ordnungsgemäß und hinreichend vor menschlichem und technischem Versagen sowie Naturkatastrophen zu schützen.

Hierbei gilt es vor allem die Grundeigenschaften der Informationssysteme bzgl. Informationssicherheit zu sichern. Bei den fundamentalen Grundeigenschaften wird zwischen den semantischen Dimensionen der Verlässlichkeit und der Beherrschbarkeit differenziert. Erstere umfasst die Sicherheit der Informationen und Daten, wobei grundlegend die drei Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität genannt werden. Beherrschbarkeit beschreibt dagegen die Sicherheit der betroffenen Kunden, Lieferanten und Mitarbeiter und unterscheidet als semantische Dimensionen die Revisionsfähigkeit sowie die Zurechenbarkeit[10].

Um reibungslose und ordnungsgemäße Prozesse sicherstellen zu können, muss im Rahmen der IT-Governance ein IT-Sicherheitskonzept in einer Organisation vorhanden sein. Ein ganzheitliches IT-Sicherheitskonzept umfasst neben der technischen Sicherheit auch die juristische, wirtschaftliche und organisatorische bzw. personelle Sicherheit. Um vertrauliche Daten, wichtige Betriebseinrichtungen und auch die Organisationsmitglieder zu schützen, investieren Organisationen erheblich in sicht- und fassbare technische Lösungen. Isoliert betrachtet, greifen derartige Maßnahmen zu kurz, denn durch fehlerhaftes Verhalten einzelner Mitarbeiter

[8] vgl. Sury (2005), S. 70
[9] vgl. Schumacher (2008), S. 16
[10] vgl. hierzu Breitner (2005), S. 24

kann jede noch so effektive technische Sicherheitsmaßnahme wertlos werden[11]. Der Mensch als Entscheider, Einkäufer, Betreiber, Nutzer, Angreifer und Verteidiger wird das entscheidende Glied in der Sicherheitskette. Eine kontinuierliche gedankliche Reflexion eines Mitarbeiters mit potenziellen Risiken, die sich im Umgang mit der IT im täglichen Arbeitsprozess ergeben können, ist dabei unabdingbar. Sicherheitsprobleme werden primär durch Irrtum und Fahrlässigkeiten eigener Mitarbeiter verursacht[12], die sich auf mangelndes Wissen und eine unzureichende Ausbildung zurückführen lassen. Ein erhöhtes Sicherheitsbewusstsein wird somit mit höherer Aufmerksamkeit, intensiverer Konzentration, größerer Achtsamkeit und Motivation gleichgestellt[13]. Das Sicherheitsbewusstsein bildet die Grundlage für sicherheitskonforme Verhaltensweisen, wobei speziell das Wissen, wie in einer Risikosituation regelkonform vorzugehen ist, ausschlaggebende Bedeutung zukommt[14].

Die Praxis zeigt durch die Vielzahl an Fachpublikationen, dass die Notwendigkeit eines hohen Sicherheitsbewusstseinsniveaus zur Schaffung einer hinreichenden personellen IT-Sicherheit bereits erkannt wurde[15]. Bei der Frage nach der Generierung von Sicherheitsbewusstsein herrscht jedoch Größenteils Uneinigkeit. Nicht selten wird Sicherheitsbewusstsein mit gewöhnlichen Schulungen gleichgesetzt, indem Sicherheitsbedürfnisse eines Unternehmens unüberlegt mit der radikalen „get the trainers in“ Methode befriedigt werden sollen[16]. Trotz hohen finanziellen Einsatzes versprechen derartige Methoden nur temporäre oder geringe Erfolgsquoten. Notwendiges Wissen, unternehmensindividuelle IT-Risiken korrekt einschätzen zu können, kann durch Schulungen durchaus vermittelt werden. Ob jedoch die notwendige Akzeptanz der Maßnahmen und die Motivation, das Wissen tatsächlich anzuwenden, vorhanden sind, bleibt zu bezweifeln[17].

Aus diesem Grund ist im Rahmen einer Security Awareness Kampagne zunächst ein Wissensgenerierungsprozess anzuregen, um auf der Mitarbeiterebene ein grundsätzliches Verständnis für sicherheitskonforme Veränderungen im Umgang mit der IT herbeiführen zu können. Die notwendige Akzeptanz und die damit tatsächliche Umsetzung kann nur durch eine gezielte Anregung der Motivation erfolgen, was die Kenntnis der Wesensmerkmale eines Menschen erfordert. Dies soll durch die folgenden Kapitel analysiert werden.

3 Menschen in Unternehmen und Organisationen

Um einer nachhaltigen personellen IT-Sicherheit gerecht zu werden, ist auf die Lernfähigkeit jedes Organisationsmitgliedes einzugehen. Tief greifende pädagogische Ansätze sind für die Planung und Durchführung eines effektiven Benutzertrainings von enormer Bedeutung. Hierbei ist die Erkenntnis des Managements, nach welchen konkreten Gesetzesmäßigkeiten Lernen funktioniert, stattfindet und unterstützt werden kann, essenziell.

[11] vgl. Zerr (2007), S. 519
[12] vgl. Pokoyski (2006), S. 61
[13] vgl. Lenz (2007), S. 26
[14] vgl. Temme (2004), S. 10
[15] vgl. bspw. Fox/ Kaun (2005), Temme (2004), Helisch (2008), Dewitz/ Jürgens (2008)
[16] vgl. Goucher (2008a), S. 12
[17] vgl. Helisch (2008)

3.1 Pädagogische Wissenssteuerung

Menschliches Lernen stellt grundlegend eine relativ andauernde Veränderung in der Verhaltensdisposition dar[18]. Jedes Organisationsmitglied agiert individuell als Wertungssubjekt, welches objektive Zustände wahrnimmt, evaluiert und mit in ihm inhärenten Vorstellungen des Idealzustandes vergleicht. Mithilfe eines Lernprozesses sollen heute noch nicht zu bewältigende Gegebenheiten und Probleme antizipierbar, berechenbar und somit lösbar gemacht werden[19]. So sollen auch unbekannte Bedrohungen, die sich bspw. über den E-Mail Verkehr ergeben können, von einem sicherheitsbewussten Mitarbeiter kritisch hinterfragt werden, bevor ein Risiko für das IT-System eingegangen wird. Gleichzeitig darf aber auch kein grundsätzliches Misstrauen entstehen, sodass Arbeitsprozesse nur noch eingeschränkt bzw. mit zeitlicher Verzögerung ausgeführt werden können und somit ein erheblicher Schaden für eine Organisation entstehen kann. Dies unterstreicht die Heranziehung pädagogischer Elemente, die das Management einer Security Awareness Kampagne gezielt einzusetzen hat, um Sicherheitsbewusstsein auch effizient fördern zu können.

Dazu sollen die drei großen Lernparadigmen des Behaviorismus, des Kognitivismus und des Konstruktivismus ausgewählte Gestaltungsempfehlungen für die Umsetzung geben. Behavioristische Ansätze gehen von einem objektiven Lernzusammenhang aus, demzufolge nach einem Input eines konkreten Gesetzes entsprechend eine bestimmte Reaktion folgt. Nach Maßgabe des Prinzips der operanten Konditionierung wird davon ausgegangen, dass ein bestimmtes Verhalten bei positiven Konsequenzen bekräftigt wird, während es bei negativen Konsequenzen zu einer Reduktion eines gelernten Verhaltens kommen kann[20]. Dabei ist wichtig, dass eine Rückmeldung unmittelbar nach einem Verhalten erfolgt, um dem Lernenden den unmittelbaren Zusammenhang erkennen zu lassen[21]. Hieraus folgt, dass Reizsituationen und deren Konsequenzen so zu gestalten sind, dass die erhofften Ergebnisse des Lernens eintreten und gefestigt werden[22]. Behavioristische Annahmen werden heute vor allem durch das E-Learning und Blended-Learning fokussiert, bei denen bspw. Trainingsprogramme eine Übung bis zur korrekten Lösung wiederholen lassen können.

Die Ansätze des Kognitivismus betrachten den Lernenden als Individuum, welches sensorische Reize aktiv und selbstständig verarbeitet. Dabei wird jede Information mit dem Gedächtnis abgeglichen und durch das vorhandene Wissen interpretiert. Die menschliche Wahrnehmung wird als aktive Konstruktionsleistung gesehen, die Informationen in selektiver Weise wahrnimmt, interpretiert und verwertet[23]. Nach den Ansichten des Kognitivismus geht es weniger um richtige oder falsche Verhaltensweisen, sondern mehr um gezielte Informationsverarbeitungs- und Problemlösungsmethoden. Dem Informationsvermittler wird eine aktive Rolle zugesprochen, die sich auf die didaktische Aufbereitung von Inhalten und Problemen bezieht, um den Informationsverarbeitungsprozess zu erleichtern. Der Lernprozess soll vom

[18] vgl. Weinberg (1999), S. 84
[19] vgl. Baitsch (1999), S. 254
[20] vgl. Skinner (1982)
[21] vgl. Kerres (2001), S. 57
[22] vgl. Reinmann (2005), S. 158
[23] vgl. Röll (2003), S. 114f.

Lehrenden initiiert, gesteuert und verbessert werden[24]. Tutorielle Systeme, die das Lernangebot an den aktuellen Wissensstand des Nutzers anpassen, sind ein Beispiel für den Einsatz kognitiver Prinzipien in der computergestützten Lerntheorie und stellen auch für eine IT-Sicherheitsschulung ein probates Mittel dar[25]. Weiterhin sind einfache Präsenzschulungen und Präsentationen frontale Lehrformen, die den kognitiven Ansätzen folgen.

Eine weitere wichtige Theorie ist der sozial-kognitive Ansatz („Lernen am Modell"). Demnach können bestimmte Verhaltensweisen nicht nur durch eigenes Handeln erlernt werden, sondern auch durch Beobachtung und Imitation verschiedener Vorgänge[26]. Dies ist besonders in Unternehmen ein wichtiger Aspekt, bei denen Mitarbeiter entsprechend den beobachteten Verhaltensweisen anderer Mitarbeiter oder Führungspersonen das eigene Verhalten anpassen.

Konstruktivistische Ansätze gehen von einer individuellen Wissenskonstruktion aus, bei denen anhand des Vorwissens, kognitiver Strukturen sowie Überzeugungssysteme Informationen aktiv interpretiert werden. Lernen wird als selbst gesteuerter Prozess betrachtet, der nicht von außen gelenkt wird, aber angeregt oder gestört werden kann[27]. Der Informationsvermittler übernimmt eine Rolle, in der es darum geht, Aktivitäten anzuregen und zu begleiten und eine Unterstützung bei der Identifikation und Lösung komplexer Problemstrukturen einzuleiten. Dies kann in direkter Weise mittels Kommunikation und Kooperation oder indirekt durch die Gestaltung von Kontexten erfolgen[28]. Weiterhin sollen Lernumgebungen und Lernpartnerschaften eingesetzt werden, wodurch es zu einer emotionalen und sozialen Einbindung des Lernenden kommt[29]. Aus dem Gesichtspunkt der Trainingsgestaltung sind Lehrinhalte auf die Interessen und Vorerfahrungen der Nutzer auszurichten, damit auch der Spaß am Erlernen nicht vernachlässigt wird.

[24] vgl. Reinmann (2003), S. 160f.
[25] vgl. Röll (2003), S. 116
[26] vgl. Reinmann (2005), S. 151
[27] vgl. Reinmann (2003), S. 162
[28] vgl. Reinmann (2003), S. 163
[29] vgl. Röll (2003), S. 119

Unterscheidungs-merkmal	Behaviorismus	Kognitivismus	Konstruktivismus
Lernauffassung	• Reizsteuerung • Formbarkeit durch Belohnung oder Bestrafung	• Verarbeitung von Informationen über sensorische Reize • Speicherung	•Individuelle und soziale Wissenskonstruktion • Selbstorganisation
Wissen wird	• abgelagert	• verarbeitet	• konstruiert
Aufgabe der Lehr-person	•Reizsituationen und Konsequenzen schaffen • systematische Lehrplanungen, konsequente Lernkontrollen	• didaktische Aufbereitung von Lehrinhalten und Problemen • Problemlöseprozesse unterstützen, Lernen initiieren	•Identifikation und Lösung komplexer Problemstrukturen • Bereitstellung verschiedener Kontexte, Lernprozesse begleiten
Lehrperson ist	•Experte	• Tutor	•Coach
Einsatz über digitale Medien	• E-Learning-Trainingsprogramme mit vorgegebenen Übungen	• Tutorielle Systeme	• diverse Werkzeuge zur Unterstützung des Lernprozesses
Paradigama	• Stimulus-Response	•Problemlösung	•Konstruktion
Lernziele	• richtige Antworten	• richtige Methoden zur Antwortfindung	• komplexe Situationen bewältigen
Philosophie	• reiner Objektivismus	• vermehrter Zugang zum Subjektivismus, Objektivismus vorherrschend	• starke Tendenz zum Subjektivismus

Tabelle 1 Unterscheidung der Lehrparadigmen in ihren Ausprägungen

Jeder der einzelnen Lerntheorien liegt ein konkretes Menschenbild zugrunde, nach denen sie jeweils entwickelt wurden. In der Praxis sind die drei grundlegenden Lerntheorien für bestimmte Teile der Kampagne brauchbar einzusetzen. Lernen kann dabei nicht als statische Angelegenheit angesehen werden, sondern ist als ein dynamischer Entwicklungsprozess zu verstehen.

Wissen als einzelne Disziplin muss allerdings nicht notwendigerweise eine tatsächliche Verhaltensänderung nach sich ziehen. Die Verhaltenskomponente im Sicherheitsbewusstsein der Mitarbeiter ist gezielt durch Motivation anzuregen. Zu diesem Zweck sind die Wesensmerkmale und typischen Verhaltensmuster eines Organisationsmitgliedes zu identifizieren und zielgerichtet zu sicherheitsbewusstem Verhalten zu lenken. Dies unterstreicht somit die Heranziehung von in der Organisationstheorie angewandten Menschenbildern.

3.2 Theorie pluralistischer Menschenbilder

Jede Organisation trägt ein individuelles Menschenbild. Menschenbilder dienen primär der Komplexitätsreduktion[30], was durch Verallgemeinerungen von Wesensmerkmalen und typisch auftretenden Verhaltensmustern in Organisationen geschieht[31]. Ein anerkannter Vertreter der Theorie pluralistischer Menschenbilder ist u.a. *Edgar Schein*[32]. *Schein* entwickelte vier grundlegende Menschenbildtypen nach ihrer historischen Entwicklung und benannte diese als „rational-economic man“, „social man“, „self-actualizing man“ und „complex man“.
Beim „rational-economic man“ gilt der Mensch als passives Wesen, dessen Empfindungen irrational sind und der verantwortungsscheu agiert, da Arbeit als mühevoll und anstrengend

[30] Vgl. Scholz (1994), S.401
[31] Vgl. Weinert (1995), S.1495
[32] Schein, Edgar (geb. 1928 in Zürich), Professor für Organisationspsychologie und Management am Massachusetts Institute of Technology (MIT) /Cambridge U.S.A.

eingestuft wird. Er strebt nach einer eigenen Nutzenmaximierung und handelt nach der Maxime des größten Gewinns[33]. Um den rationalen Interessen einer Organisation nicht entgegenzustehen, ist eine strenge Führung unter stetiger Kontrolle unumgänglich.

Diverse Studien konnten allerdings widerlegen, dass soziale Beziehungen am Arbeitsplatz eine Auswirkung auf die Leistung haben kann[34]. So entwickelte sich allmählich der zweite Menschenbildtypus, bei dem der Mensch als soziales Wesen verstärkt nach sozialen Kontakten strebt. Arbeit wird beim „social man" als sinnentleerend aufgefasst, so dass primär soziale Kontakte eine Ersatzbefriedigung geben[35]. Durch soziale Beziehungen in Form von Kommunikation sowie durch die Zusammenarbeit in Gruppen am Arbeitsplatz erhält der „social-man" ein zunehmendes Zugehörigkeitsgefühl sowie den Willen der Integration in die Organisation. Eine materielle Belohnung steht dabei nicht im Vordergrund[36].

Im weiteren Zeitverlauf erfolgte die Erkenntnis, dass der Mensch nach Selbstverwirklichung strebt, sodass sich das Menschenbild des „self-actualizing man" entwickelte. Der Mensch ist zu einer Weiterentwicklung am Arbeitsplatz fähig, was nur möglich ist, wenn autonome Entscheidungen getroffen werden können. Dabei muss es nicht notwendigerweise zu einem Konflikt zwischen den individuellen und den organisationalen Zielen kommen. Vielmehr werden die Organisationsmitglieder versuchen ihre Ziele mit denen der Organisation abzustimmen[37]. Eigenmotivation, Selbstkontrolle, die Übernahme von Verantwortung und die Weiterentwicklung durch den Arbeitsprozess stehen somit bei diesem Menschenbildtypus klar im Vordergrund[38].

Auf Grund fehlender Aussagefähigkeit bzgl. der Anwendbarkeit eines konkreten Menschenbildes in der Praxis, entwickelte *Schein* das Menschenbild des „complex man", indem er die Grundannahmen der vorherigen Menschenbilder zu einem Grundmenschenbild zusammenfasste. Nach *Schein* gilt der Mensch heute als komplexes Wesen, der äußerst wandlungs- und anpassungsfähig ist. Weiterhin geht er von inter- sowie intraindividuellen Unterschieden der Bedürfnisse von Organisationsmitgliedern aus[39]. Der Mensch lernt dauerhaft dazu und kommt durch Erfahrungen stetig zu neuen bzw. veränderten Motiven[40]. Weiterhin kann ein einzelner Mitarbeiter in verschiedenen Unternehmensbereichen unterschiedliche Motive verfolgen.

Diese Ansicht lässt darauf schließen, dass der Mensch situations-, typ-, oder altersbedingt besonders passiv agieren oder nach sozialen Kontakten oder mehr Autonomie streben kann, d.h. auch wenn *Schein* den Menschen heute als komplexes Wesen ansieht, schließt er die Gültigkeit der übrigen Menschenbilder nicht kategorisch aus. Ein verallgemeinertes Führungsverhalten kann es beim „complex man" nicht geben. Vielmehr ist, im Bezug auf die Förde-

[33] vgl. Kirchler et al. (2008), S. 28
[34] vgl. Kirchler et al. (2008), S. 64
[35] vgl. Staehle (1999), S. 194f.
[36] vgl. Kirchler et al. (2008), S. 63
[37] vgl. Kirchler et al. (2008), S. 96
[38] vgl. Staehle (1999), S. 195f.
[39] vgl. Kirchler et al. (2008), S. 127
[40] vgl. Staehle (1999), S. 195f.

rung des IT-Sicherheitsverhaltens, ein Anreizsystem zu konzipieren, welches unter Beachtung des Menschenbildes auf die individuellen Präferenzen der Mitarbeiter ausgelegt ist. Nur dadurch kann gewährleistet werden, dass jedes Organisationsmitglied durch präferierte Anreize angesprochen und motiviert wird.

3.3 Integration umfassender Anreizsysteme

Ohne die Schaffung von Anreizen zur Anregung der Motivation lassen sich während und vor allem nach einem Training nur schwer nachhaltige Verhaltensänderungen erzielen und die erwünschte Wirkung wird verfehlt. Das Verhalten eines Mitarbeiters muss durch den Einsatz verschiedener Anreize gezielt gesteuert werden, um dauerhaft ein auf die Sicherheit bedachtes Auftreten innerhalb einer Organisation zu gewährleisten und die tatsächliche Anwendung des erlernten Wissens zu bewirken. Aus diesem Grund muss ein umfassendes leistungsbezogenes Anreizsystem innerhalb eines Unternehmens implementiert werden.

Anreize sollen dazu führen, dass die Motive (Verhaltensbereitschaften) eines Menschen zu einem bestimmten zielgerichteten Verhalten gelenkt werden[41], was als Motivation bezeichnet wird. Eine gängige Unterscheidung wird zwischen extrinsischer und intrinsischer Motivation vorgenommen. Dabei wird von einer intrinsischen Motivation gesprochen, wenn „motiviertes Verhalten unter der Kontrolle des Handelnden selbst liegt“[42]. Demzufolge gilt ein Mitarbeiter als intrinsisch motiviert, wenn dieser aus der eigenen Tätigkeit heraus eine Befriedigung erzielt.[43]. Die erfolgreiche Ausführung einer Tätigkeit bringt dabei den notwendigen Spaß an der Arbeit[44]. Extrinsische Motive hängen von Verstärkern, die von außen zugeführt werden, ab[45]. Im Allgemeinen wird zwischen immateriellen und materiellen Motiven unterschieden, wobei ersteres bspw. den Wunsch nach Sicherheit, Kontakten oder Karriere betrifft, während letzteres bspw. monetäre Zusatzleistungen darstellen (vgl. Abbildung 1)[46].

[41] vgl. Becker (1990), S.9
[42] siehe Mietzel (2007), S. 349
[43] vgl. Staehle (1999), S. 165
[44] vgl. Mietzel (2007), S. 349
[45] vgl. Staehle (1999), S. 166
[46] vgl. Becker (1990), S. 10

BETRIEBLICHE ANREIZE	POSITIVE	intrinsische	immateriell	eigenwertige	- von der Arbeit selbst ausgehend - von den Handlungszielen ausgehend - wechselseitige Stimulanz von Können und Wollen im Arbeitsprozess
				ethische	- unternehmensethische Reflexionen
		extrinsische	immateriell	soziale	-Führungsverhalten, vorbildliche symbolische Führung, Partizipation, Kommunikation, etc.
				organisatorische	-Unternehmensimage, Arbeitszeitsystem, Unternehmenskultur, Karriereanreize, Identifikation/ Commitment etc.
			mat.	direkte	- Entlohnung, Prämienzahlungen, Erfolgsbeteiligungen, etc.
				indirekte	- Firmenwagen, Essensgutscheine, USB-Sticks,…
	NEG.				- betriebliche Haftungsregelungen - betriebliche Disziplinarmaßnahmen - sichtbare Kontrollen

Abbildung 1 Betriebliche Anreize im Überblick. Quelle: in Anlehung an Gurtner et al. (2007), S. 16; Seidel (1991), S. 183

Wesentlich ist die Verknüpfung des Anreizsystems mit den betrieblichen Zielen, so dass das Verhalten eines Mitarbeiters entsprechend dem im Unternehmen vorherrschenden Menschenbild systematisch beeinflusst werden kann. Entsprechend der behavioristischen Lerntheodie gelten positive extrinsische und vor allem negative Anreize als primäre Motivationsfaktoren[47]. Gemäß dem Reiz-Reaktions-Modell wird ein Verhalten verstärkt, wenn unmittelbar nach einer Reaktion eine Belohnung erfolgt. Um Erfolg zu erzielen muss die Belohnung für den Menschen klar ersichtlich sein, sodass Größenteils materielle Anreize zu setzen sind. Entgegengesetzt muss zur Verminderung eines bestimmten Verhaltens auf das Prinzip der Bestrafung gesetzt werden, was durch das Aussenden negativer Anreize erfolgt. Kognitive Lerntheorien tendieren von der Denkhaltung des Objektivismus zu mehr Subjektivismus und sind somit als Zwischenstufe beider aufzufassen. Aus diesem Grund sind bereits erste Ansätze zur intrinsischen Motivation erkenntlich. Der Schwerpunkt der Motivation liegt allerdings nach wie vor auf eine extrinsische Motivation. Dabei ist die Anreizart auf den Lernenden in der jeweiligen Lernsituation anzupassen. Konstruktivistische Lerntheorien setzen den Fokus der Motivation auf nachhaltiges Lernen, die eine intrinsische Motivation voraussetzt. Hierbei ist eine für den Lernenden empfundene angenehme Lernatmosphäre ebenso, wie die richtige Wahl des gewählten Themas oder die Bedeutsamkeit der Aufgabenstellung wichtig, um zu

[47] vgl. Mietzel (2007), S. 352

einer steigenden intrinsischen Motivation die Nachhaltigkeit des Lernens anzuregen[48]. Weiterhin wichtig ist die Einbindung der Mitarbeiter in Entscheidungen über die Relevanz, Bedeutsamkeit und Wichtigkeit der pädagogischen Prozesse, damit selbstbestimmter der eigenen Tätigkeit nachgegangen wird. Mit der selbstständigen Arbeit in Gruppen wird neben dem Bedürfnis der Selbstbestimmung ebenfalls dem Bedürfnis nach sozialen Kontakten gerecht, sodass auch extrinsische Anreize von ausschlaggebender Bedeutung sind.

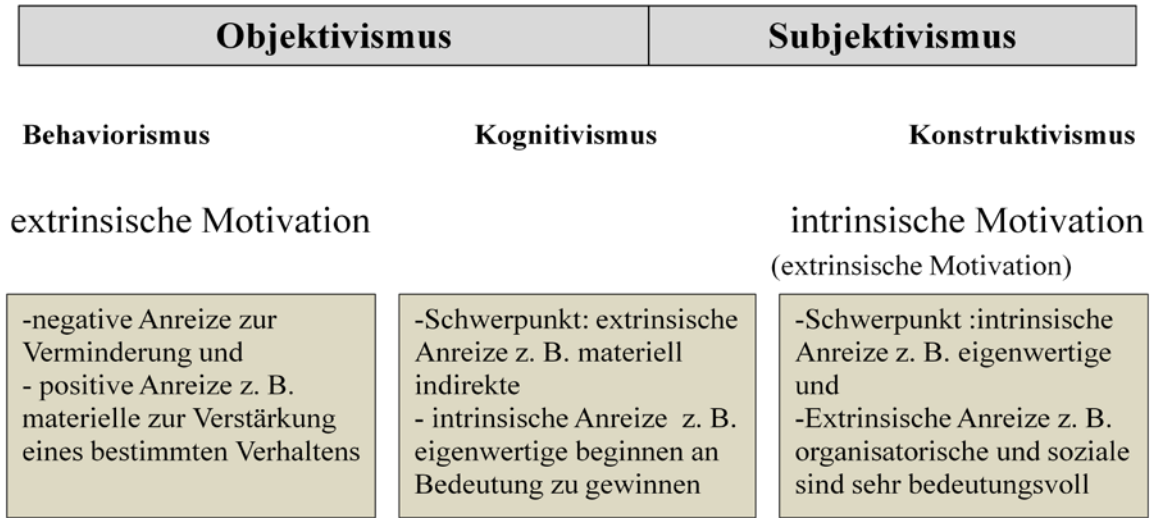


Abbildung 2 Anreizschwerpunkte in den Lerntheorien

Auf organisationaler Ebene gilt vor allem die Arbeitszufriedenheit als ein entscheidender Faktor intrinsischer Motivation. Zufriedene Mitarbeiter verfügen meist über eine höhere Leistungs- und Einsatzbereitschaft, wenn sie sich mit der Organisation, Teilen der Organisation oder den zu bewältigen Aufgaben identifizieren können[49]. Verspüren Mitarbeiter keine Verpflichtung ihrem Arbeitgeber gegenüber, so mangelt es an einer emotionalen Bindung, die schließlich zu einer „inneren Kündigung" führen kann. Eine hohe Unternehmensidentifikation führt folglich zu einer Akzeptanz der Normen und Wertvorstellungen, die in einer Organisation gelebt werden[50].

Unter Beachtung des schwerpunktmäßigen Einsatzes einer spezifischen Lehrform ist weiterhin ein Anreizsystem auf das vorherrschende Menschenbild auszulegen. *Schein´*s Menschenbilder lassen eindeutige Motivationsmuster erkennen. Der „rational-economic man" ist primär durch monetäre Anreize motivierbar. Die zentrale Aufgabe des Managements bei diesem Menschenbild ist strenge Kontrolle, um das Mitarbeiterverhalten genau beobachten zu können. Der Einsatz negativer Anreize wird ein entscheidender Faktor.

Beim „social man" bilden kommunikative und zwischenmenschliche Beziehungen und auch die Teilnahme an Entscheidungsprozessen die wichtigsten immateriellen Anreizarten. Bei dieser Art von Menschentyp muss der Fokus auf soziale Anreize ausgeweitet werden, indem z. B. Gruppenarbeit gefördert wird. Innerhalb einer Gruppe kann Druck auf einen Einzelnen ausgeübt werden, der nicht dieselbe Anstrengung und/ oder Leistung bringt, wie der Rest der Gruppe.

[48] vgl. Siebert (2005), S. 35
[49] vgl. Becker (2008), S. 125
[50] vgl. von der Ruhr/ Bosse (2006), S. 400

Der „self-actualizing man“ wird primär intrinsisch motiviert, wobei externe Entlohnungssysteme eine passive Anpassung bewirken und zu einer Behinderung der Selbstentfaltung werden können. Die Funktion der Führungskräfte liegt primär im anregen, unterstützen und fördern der Mitarbeiter. Dies ist vor allem durch eine verstärkte Delegation möglich, wodurch Beschäftigte ihre Tätigkeiten als sinnhaft empfinden, was wiederum eine verstärkte Identifikation hervorrufen kann. Besonderes Augenmerk liegt in den Arbeiten, die für den einzelnen Mitarbeiter als herausfordernd und befriedigend gelten müssen[51].

Die Gestaltung von Anreizen beim „complex man“ ist komplexer als bei den übrigen Menschenbildern. Auf Grund der ständigen erfahrungsbedingten Veränderungen und Anpassungen der Motive muss ein individuelles Maß an Anreizen gesetzt werden, die sich situationsbedingt ändern. Führungspersonen agieren somit als Diagnostiker von Situationen, die Unterschiede erkennen und ihr eigenes Verhalten situationsbedingt variieren[52]. Es gilt die individuellen Bedürfnisse der Mitarbeiter zu identifizieren und auf das Führungsverhalten anzupassen. Die hohe Flexibilität eines Anreizsystems ist als besonders wichtig zu betrachten, um dauerhaft den verschiedenen Gegebenheiten stand zu halten[53].

Menschenbilder	**Eigenschaften**	**Anreizarten**	**Führungsverhalten**
rational-economic man	- Passivität - Verantwortungsscheue - Nutzenmaximierung	- monetäre Anreize - negative Anreizsysteme	- strikte und verantwortungsbewusste Führung - oberstes Kontrollorgan
social-man	- verstärkte soziale Bedürfnisse - Arbeit ist sinnentleert, soziale Kontakte geben Ausgleich	- soziale Anreize - Abkehr von reinen materiellen Anreizen	- Berücksichtigung sozialer Bedürfnisse - Integration in die Gruppe - Kommunikation
self-actualizing man	- Streben nach Selbstverwirklichung und Autonomie - Fähigkeit zur Weiterentwicklung - Eigenmotivation, Selbstkontrolle	- intrinsische Anreize - externe Entlohnungssysteme vernachlässigbar	- Förderung und Unterstützung der Mitarbeiter - Anregung der intrinsischen Motivation - verstärkte Delegation
complex man	- Komplexität durch Anpassungs- und Wandlungsfähigkeit - dauerhafte Weiterbildung - Veränderung der Motive	- individuell angepasste Anreizsysteme	- Identifikation der individuellen Bedürfnisse - situative Führung - es existiert keine verallgemeinerte Führungsstrategie

Tabelle 2 Menschenbilder, Anreizarten und entsprechendes Führungsverhalten. Quelle: in Anlehnung an Scholz (1994), S. 407, deutlich erweitert durch den Autor

[51] vgl. Kirchler et al. (2008), S. 97
[52] vgl. Schein (1980), S. 55f.
[53] vgl. Becker (1990), S. 8f.

4 Handlungsempfehlungen zur nachhaltigen Mitarbeitersensitiven Umsetzung von IT-Sicherheit – ein 5-Phasen Modell

Nachdem die verschiedenen Lerntheorien und Menschenbilder sowie deren Unterschiede in der Motivierbarkeit skizziert wurden, werden in den folgenden Kapiteln die Ergebnisse zu Handlungsempfehlungen für ein umfassendes Risikomanagement zusammengefasst. Die nachhaltige Generierung von Sicherheitsbewusstsein kann nur innerhalb einer umfassend geplanten und durchgeführten Kampagne vollzogen werden, um auf die Komplexität der Organisationsmitglieder reagieren zu können. Der Gesamtprozess einer Kampagne ist in fünf Phasen zu untergliedern, beginnend mit einer Grundphase, die richtungsweisend für die vier weiteren Managementphasen – Identifikation, Design, Umsetzung und Evaluation – ist. Jede einzelne Phase beginnt mit einer Methodenauswahl und der damit einhergehenden Analyse eingesetzter Lerntheorien. Darauf aufbauend werden die in jeder Phase einsetzbaren Anreizarten diskutiert.

4.1 Phase 1 – Grundvoraussetzungen schaffen

Zu Beginn einer jeden Kampagne müssen drei wesentliche Faktoren Berücksichtigung finden: die Identifikation und Förderung der IT-Sicherheitskultur, der Management-Support sowie die Berücksichtigung kultureller Unterschiede.

Für den Erfolg einer Security Awareness-Kampagne ist eine ausgebildete IT-Sicherheitskultur maßgeblich. Die Einhaltung von IT-Sicherheitsmaßnahmen muss für jedes Organisationsmitglied gleichermaßen zu einer Selbstverständlichkeit werden, wie zum Beispiel Sicherheitsmaßnahmen auf Baustellen und Industrieanlagen. *Scheins* Ansichten über eine ausgeprägte Organisationskultur lassen sich ideal für eine Analyse der IT-Sicherheitskultur nutzen[54]. Nach *Schein* bilden Artefakte die obere und gleichzeitig sichtbare Ebene, die sich durch gezielte Maßnahmen logisch verändern und beeinflussen lassen. Auf der Basis einer ausgeprägten IT-Sicherheitskultur deuten physische Sicherheitsmaßnahmen, wie etwa der beschränkte Zugang zu sensiblen Bereichen eines Unternehmens für einen vordefinierten Personenkreis oder auch Sensibilisierungsmaßnahmen, auf den hohen Stellenwert der Sicherheit einer Organisation hin. Artefakte sind zwar objektiv beobachtbar, werden allerdings subjektiv interpretiert[55]. Aus diesem Grund sind besonders die sichtbaren Elemente einer IT-Sicherheitskultur derart eindeutig auszulegen, dass es zu keiner subjektiven Fehlinterpretation kommen kann und die Bedeutsamkeit von jedem Organisationsmitglied wahrgenommen und akzeptiert wird. Um eine korrekte subjektive Wahrnehmung der Organisationsmitglieder zu sichern, sollte die Bedeutung der Artefakte mit den Mitarbeitern abgesprochen und deren zugrunde liegenden Muster richtig dargestellt werden. Dabei sind sowohl schriftliche und verbale Ausdrucksformen als auch das sichtbare Verhalten der Organisationsmitglieder[56] und der Managementebene bedeutende Merkmale um Artefakte lebendig zu gestalten. Dabei dienen niedergeschriebe-

[54] vgl. Kirchler et al. (2007), S. 158
[55] vgl. Kirchler et al. (2007), S. 158
[56] vgl. Kirchler et al. (2007), S. 158

ne Verhaltenskodexe, Standards und Informationen zur IT-Sicherheit sowie vertragliche Vereinbarungen (bspw. zum Umgang mit betrieblichen USB-Sticks sowie Plakate und Broschüren) dazu, die IT-Sicherheit innerhalb einer Unternehmenskultur sichtbar umzusetzen.

Die mittlere Ebene einer IT-Sicherheitskultur bilden die Werte und Normen, die als teils sichtbar und teils unsichtbar zu klassifizieren sind[57]. Sie werden von der Managementebene gelebt bzw. von den Organisationsmitgliedern geprägt[58]. Maxime, ungeschriebene Verhaltenskodexe und Verbote, die die Organisationsmitglieder in einem breiten Umfang teilen, formen hierbei die Sicherheitskultur. Die Strategien, Philosophien und Verhaltensweisen sind dabei gezielt auf sicherheitskonformes Verhalten auszulegen, um eindeutige Interpretationsmuster bei den Unternehmensmitgliedern zu erhalten. Besonders Verbote und Sanktionen sind im Rahmen von Sicherheitsmaßnahmen ein wichtiges Element, um Normen lebendig werden zu lassen.

Die Basisannahmen, aus denen sich die Werte und Normen ableiten lassen, die sich wiederum in der sichtbaren Ebene widerspiegeln, prägen auf unsichtbare Weise das organisatorische Handeln. Sie haben sich zu selbstverständlichen Orientierungspunkten etabliert, die automatisch von jedem Organisationsmitglied, ohne darüber nachzudenken oder sie gar zu kennen, akzeptiert und verfolgt werden. Besonders die Einstellungen im Bezug auf das Menschenbild, die daraus resultierenden Motivationsstrukturen und die Ansichten des menschlichen Handelns prägen die Basisannahmen sowie die gesamte Kampagne. Ein besonderes Augenmerk sollte auf zwischenmenschliche Beziehungen gesetzt werden. Entsprechend konstruktivistischer Auffassungen des Lernens nehmen soziale Beziehungen und Kommunikation einen hohen Stellenwert ein. Aus diesen Gründen müssen zwischenmenschliche Beziehungen gezielt verbessert werden. Beziehungsstörungen gilt es zu eliminieren, um eine völlige Deformation, der später zu vermittelten Inhalte, zu verhindern. Fehlt es bspw. an Wertschätzung gegenüber den Beschäftigten, so kann ein inhaltlich noch so gutes Awareness-Konzept seine Wirkung verfehlen, weil eine Demotivation infolge mangelnder Identifikation zu Akzeptanzproblemen führen kann.

Die Sicherheitskultur darf nicht als völlig statisches Gebilde betrachtet werden[59]. Eine Security Awareness Kampagne führt nicht nur zu einer Veränderung der IT-Sicherheitskultur, sondern auch die IT-Sicherheitskultur an sich beeinflusst wesentlich wichtige Elemente der einzelnen Phasen einer Security Awareness Kampagne. Es kann demnach von einer wechselseitigen Abhängigkeit zwischen Unternehmenskultur und Sensibilisierungskampagne gesprochen werden. Aus diesem Grund bringt eine Unternehmenskultur bereits einen gewissen Grad an Sicherheitsbewusstsein mit, den es zu identifizieren und zu verbessern gilt.

Im engen Zusammenhang mit der Förderung der gelebten Werte in einem Unternehmen steht auch der Management-Support in einer Security Awareness Kampagne. Der Entscheidungsträger einer Organisation muss ein Verständnis für den Risikofaktor Mensch generieren, verstehen welche Risiken und Herausforderungen zu bewältigen sind und sich zur Förderung des

[57] vgl. Kirchler et al. (2007), S. 158
[58] vgl. Jahner/ Krcmar (2006), S. 4
[59] vgl. Helisch (2007), S. 14

IT-Sicherheitsbewusstseins bekennen[60]. Der Management-Support erzielt eine positiv beeinflussende Wirkung auf vier Schlüsselfaktoren - die Awareness-Kampagne an sich, die IT-Sicherheitskultur, die IT-Sicherheitspolicy sowie den Aspekt der Nachhaltigkeit - die auf das IT-Sicherheitsbewusstsein in einer Organisation fördernd wirken[61]. Demnach muss eine Awareness-Kampagne vom Management initiiert, durch adäquate Ressourcen unterstützt und kommuniziert werden. Die Bedeutsamkeit des Themas muss darüber hinaus durch eine aktive Teilnahme an Benutzertrainings durch das Management und v. a. durch die sichtbare und konsequente Umsetzung der Sicherheitsmaßnahmen im täglichen Arbeitsprozess unterstrichen werden. Nach sozial-kognitiver Lernauffassungen kann ein Vorgesetzter eine Unterstützung der Aufmerksamkeitsprozesse seiner Mitarbeiter bewirken, indem die Vorbildfunktion klar ausgeführt wird. Es kommt zu einem „Lernen durch [den] Beobachtungsprozess", indem versucht wird sichtbare positive Verhaltensweisen einer Bezugsperson zu reproduzieren. Die sichtbare Einhaltung erforderlicher Sicherheitsmaßnahmen durch das Management lassen eine Sicherheitskultur lebendig werden. Als weiteren Einflussfaktor muss vom Management eine klare, zielgerichtete Strategie verfolgt und mit den Unternehmenszielen übereinstimmend in eine Sicherheitspolicy etabliert werden. Um die Aktualität und Angemessenheit getroffener Maßnahmen zu gewährleisten, ist eine kontinuierliche Überwachung durchzuführen. Wichtig ist, dass die durch gezielte Maßnahmen umzusetzende Policy von den Organisationsmitgliedern tatsächlich eingehalten wird (Nachhaltigkeit). Besonders beim Aussetzen negativer Anreize hat das Management eine schwerwiegende Aufgabe zu bewältigen. Hierbei ist eine Balance zu finden, sodass die Sanktionen von den Organisationsmitgliedern nicht als zu mild bzw. extrem eingestuft werden. Die Organisationsmitglieder müssen ein Sanktionssystem zwar nicht tolerieren, trotz dessen aber die Anwendung verstehen und anerkennen.

Organisationen, die in einem multinationalen Umfeld agieren und eine unternehmensübergreifende Kampagne durchführen wollen, stehen vor der komplexen Aufgabe, kulturelle Unterschiede zu berücksichtigen. Der anerkannte Kulturwissenschaftler *Geert Hofstede,*[62] wies durch diverse Studien darauf hin, dass verschiedene Gesellschaften, kulturell bedingt, unterschiedlich auf bestimmte Faktoren reagieren[63]. In China bspw. wird in dieser Hinsicht, wenn an einem Mitarbeiter aufgrund von fehlerhaftem oder nachlässigem Verhalten richtungsweisende Kritik ausgeübt wird, keine Wirkung erzielt. Erfolgt allerdings eine Schuldzuweisung vor anderen Mitarbeitern, so empfindet dieser in der Regel Schuldgefühle und Scham. Das Verhalten des Mitarbeiters wird jedoch nicht unmittelbar nach der Kritik geändert, sondern bedarf einer gewissen Zeitspanne. Darüber hinaus werden die übrigen Mitarbeiter sich innerlich mit dem Beschuldigten solidarisieren[64]. Werden kulturelle Unterschiede nicht eingehend berücksichtigt, so kann eine standardisierte und nach nationalen Werten und Einstellungen organisierte Sensibilisierungskampagne in einem multinationalen Umfeld erhebliche Reibungsverluste erzielen oder gar in einigen Kulturen auf Ablehnung stoßen[65]. Führungsperso-

[60] vgl. Santa (2007)
[61] vgl. Knapp/ Marshall (2007), S. 54f.
[62] Hofstede, Gerard Hendrik (geb. 1928 in Haarlem), Professor für Organisationsanthropologie und Internationales Management an der Universität Maastricht/ Niederlande
[63] vgl. Hofstede (2001), S. 146
[64] vgl. Zinzius (2006), S. 58
[65] vgl. auch Helisch (2007), S. 13

nen müssen somit auch innerhalb einer Security Awareness Kampagne interkulturelle Kompetenzen aufweisen, indem kulturelle Unterschiede identifiziert und erfolgreich in die Kampagne eingebunden werden[66].

4.2 Phase 2 – Diagnose

Mit der Diagnosephase beginnt die Planung der Awareness Kampagne. Die Qualität dieser Phase bestimmen die auf ihr beruhenden Maßnahmen und damit die Effektivität des gesamten Trainings. Ausgangspunkt der Diagnosephase bildet ein umfassendes, schriftlich fixiertes IT-Sicherheitskonzept, das die notwendigen Maßnahmen zur Realisierung eines angemessenen vordefinierten Sicherheitsniveaus beschreibt und gleichzeitig als das „Soll-Konzept" einer Kampagne fungiert. IT-Sicherheitskonzepte sind in der Praxis meist komplexer Natur, so dass sie nur eine geringe Alltagstauglichkeit aufweisen[67]. Ohne notwendige Sensibilisierungsmaßnahmen und das herunter brechen auf die Mitarbeiterebene werden nur wenige Mitarbeiter Kenntnis von den Sicherheitsmaßnahmen nehmen.

Ermittlung des Status Quo

Um gezielt Wissenslücken im Sicherheitsbewusstsein der Mitarbeiter schließen zu können, ist als nächster Schritt eine Ist-Analyse durchzuführen. Diese sog. Nullmessung birgt die Vorteile, dass frühzeitig Informationen über die Inhalte einer Kampagne aufgedeckt werden und leistet im Falle einer späteren Wiederholungsdurchführung einen entscheidenden Einblick des Return on Investments[68]. Ein Instrument zur Ermittlung des Status Quo stellt u. a. die Schwachstellenanalyse dar. Im Rahmen einer Schwachstellenanalyse sollen aktuelle Wissensstände über IT-Sicherheitsmaßnahmen und damit das Niveau des Sicherheitsbewusstseins abgefragt und eingeschätzt werden. Als weiteren Prozess der Ist-Analyse sind die Motivationsfaktoren zu analysieren, auf deren Basis zu einem späteren Zeitpunkt Anreize gezielt gesetzt werden sollen. Als Initiierungsmaßnahmen sind Selbsteinschätzungsverfahren von Experten aus dem IT-Bereich und Einzelinterviews in der Form von persönlichen Gesprächen denkbare Methoden, die bspw. mit der Managementebene geführt werden können. Auch der Human Ressource Bereich kann einen sinnvollen Beitrag aus dem Bereich Mitarbeiterzufriedenheit und Kreativität leisten, der in die Kampagne ideal eingebettet werden kann.

Um eine große Masse an Mitarbeitern aus diversen Unternehmensbereichen ansprechen zu können, sollten Befragungen in schriftlicher bzw. vornehmlich in elektronischer Form durch standardisierte Formulare vorgenommen werden. Entsprechend den obigen Management-Support Ansätzen ist bereits an dieser Stelle das Management in die Kampagne einzubeziehen. Den Fragebögen könnte, um deren Wichtigkeit zu unterstreichen, eine kurze Stellungnahme des Managements zur Sicherheitsbewusstseinskampagne vorangehen. Die persönlichen Einstellungen eines Mitarbeiters zu sicherheitstechnischen Maßnahmen können durch gezielte Fragestellungen erkannt werden. Ein solcher Fragebogen sollte an den Einflussfakto-

[66] In der Führungslehre wird in diesem Zusammenhang vom Diversity-Management gesprochen. Vgl. Hentze et al. (2005), S. 542f.
[67] vgl. Dewitz/ Jürgens (2008), S. 583
[68] vgl. Zerr (2006), S. 23

ren, die auf das sicherheitsbewusste Verhalten eines Menschen wirken, orientiert sein[69]. Hierdurch ist eine Einschätzung über das Fühlen, Denken und Wissen hinsichtlich sicherheitsrelevanter Themen möglich[70]. Weiterhin sollten konkrete Fragestellungen konstruiert werden, die die Bedürfnisse der Mitarbeiter und damit motivationsrelevante Aspekte offen legen.

In Bezug auf die Motivation gilt es frühzeitig richtungsweisende Anreize in die Kampagne zu integrieren, um bei einem Mitarbeiter eine kontinuierliche Erhöhung der Motivation erreichen und damit eine grundlegende Verhaltensänderung bewirken zu können. Entsprechend dem nach *Schein* heute vorherrschenden Menschenbild des „complex man" müssen Anreize möglichst breit in die Sicherheitskampagne integriert werden, um unterschiedliche Mitarbeitertypen ansprechen zu können[71]. Durch eine erfolgreiche Einbindung eines Mitarbeiters in einzelne Elemente des Planungsprozesses kann die Motivation geweckt werden. Werden bspw. in jedem Unternehmensbereich gezielt Mitarbeiter, die bspw. nach mehr Verantwortung streben, ausgewählt und wird ihnen die Verantwortung der Bearbeitung der Fragebögen zugeschrieben, so kann dies einen intrinsischen Motivationsprozess bei diesen Mitarbeitern bewirken. Die Mitarbeiter werden von sich aus bestrebt sein, die Aufgabe erfolgreich umzusetzen.

Neben Befragungen sind auf der Mitarbeiterebene ergänzend Beobachtungen einzusetzen. *Zerr*[72] erklärt dies aus soziowissenschaftlicher Sicht durch die Einstellungs- und Verhaltenskomponente menschlichen Handelns im Umgang mit Sicherheitsmaßnahmen. Hierbei geht er davon aus, dass die gedankliche Auseinandersetzung mit potenziellen Risiken im Bereich der IT-Sicherheit in spezifische Einstellungen mündet. Diese Einstellungen stärken wiederum das sicherheitsbewusste Verhalten der Organisationsmitglieder. Sicherheitsbewusstes Verhalten kann mittels Beobachtungen identifiziert werden. Im Gegensatz dazu sind die Einstellungen nicht beobachtbar sondern nur zu hinterfragen[73]. Rundgänge durch besonders sensible Abteilungen, der Einsatz passwortgeschützter Bildschirmschoner oder die korrekte Anbringung von Notebookschlösser sind beispielhafte Szenarien, die das tägliche sicherheitsbewusste Verhalten der Mitarbeiter aufdecken können. Eine weitere Beobachtungsmethode stellt eine Analyse bereits eingetretener Schadensfälle dar. Denkbar sind die Analyse protokollierter Schadensfälle wie bspw. der Verlust von Notebooks, Handys oder Daten und die Auswertung von Log-Files.

Im Hinblick auf die Motivation bilden Beobachtungen hingegen negative Anreize. Dadurch, dass die Organisationsmitglieder eine verstärkte Kontrolle innerhalb der Organisation wahrnehmen, wird die IT-Sicherheit entsprechend dem Prinzip der Verstärkung persönlich an Stellenwert gewinnen. Allerdings sind die Wirkungen negativer Anreize umstritten[74]. Es darf bei den Mitarbeitern nicht der Eindruck erweckt werden, dass sie einer totalen Überwachung un-

[69] Schmidt bietet auf diesem Themengebiet einige interessante Handlungsempfehlungen zum Aufbau und zur Gestaltung von Fragebögen und Interviews. vgl. Schmidt (2006), S. 53ff.
[70] vgl. Zerr (2007), S. 521
[71] vgl. Kapitel 3.3
[72] Zerr, Konrad (geb. 1963 in Aachen), Professor für Marketing und Kommunikationsforschung an der Hochschule Pforzheim/ Deutschland
[73] vgl. Zerr (2007), S. 520
[74] vgl. Knapp/ Marshall (2007), S. 57

terliegen und ihnen ein geringes Vertrauen entgegen gebracht wird. Allerdings sind Beobachtungen lediglich dazu imstande das tatsächliche Sicherheitsverhalten im täglichen Arbeitsprozess zu identifizieren, sodass die Anwendung als notwendig erachtet werden kann[75].

Bewertung potenzieller Risiken

Nach der Ermittlung des Status Quo und deren Abgleich mit dem Soll-Konzept, muss aufbauend eine Einstufung der Risikosituation vollzogen werden. Eine bewährte visuelle Darstellung bietet die Erstellung einer Matrix, in der jede potenzielle Bedrohung grafisch dargestellt wird.

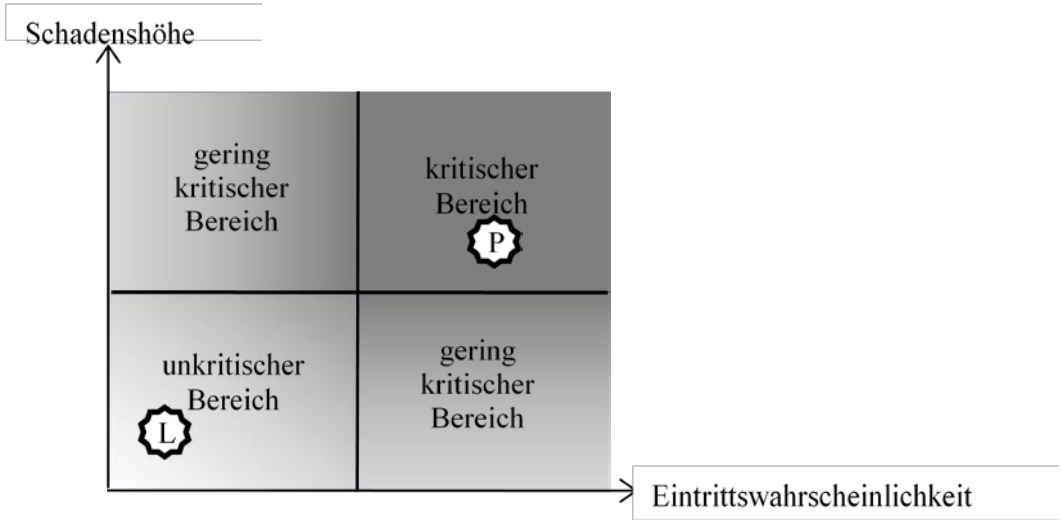


Abbildung 3 Risikobewertungsdiagramm. Quelle: in Anlehnung an Schmidt (2006), S. 118

In der Abbildung 3 wurden beispielhaft zwei mögliche Einteilungen durch sternförmige Punkte dargestellt. Der linke im unteren Quadranten liegende Punkt (L) ist als unkritisch einzustufen. Sowohl die Wahrscheinlichkeit für das Eintreten als auch die Schadenshöhe sind gering. Beispielhaft könnte es sich um das Risiko des Diebstahls eines Mitarbeiterlaptops handeln. Ein Unternehmen, in dem strenge Zugangsberechtigungen existieren und nur wenige Daten lokal auf einem Arbeitsplatzrechner oder unverschlüsselt gespeichert werden, wird diese Risikoart geringer einstufen, als ein Unternehmen, bei der auch Kundenverkehr innerhalb einiger Abteilungen herrscht. Der Punkt im oberen rechten Quadranten (P) ist als kritisch einzugliedern, mit einer potenziell hohen Eintrittswahrscheinlichkeit und einem hohen Schadensausmaß. Beispielhaft könnte es sich um die Einhaltung der Passwort-Richtlinien handeln, die nur nachlässig umgesetzt wurden und somit eine beträchtliche Schwachstelle darstellen.

Eine weitere wirksame Bewertungsmethode stellt ein Benchmarking dar, das als „Lernen von den Besten“ verstanden werden kann. Ein Benchmarking mit verschiedenen Unternehmensbereichen oder gar mit anderen Unternehmen, bei dem einzelne Prozesse eines Unternehmens mit denen eines erfolgreichen Unternehmens verglichen und abgestimmt werden, ist ein durchaus sinnvoller Prozess, um zu einer Zielbildung zu kommen.

[75] vgl. hierzu Riley (2006). Riley konnte in ihrer Studie zum Passwortverhalten zeigen, dass ein Großteil der Befragten wussten, dass ein sicheres Passwort bspw. auch Symbole und Zeichen enthalten sollte, während lediglich ein minimaler Teil der Befragten dies tatsächlich in die Tat umgesetzt haben.

Anhand dieser Bewertungsmethoden kann entschieden werden, welche Bereiche einer intensiven Sensibilisierung bedürfen und welche Bereiche bereits akzeptabel ausgeprägt sind. Der Benchmark-Ansatz ist allerdings auf seine Eignung zu prüfen, denn es besteht die Gefahr, dass es für die Ziele eines Unternehmens nicht relevant ist. Demzufolge stellt die Definition der unternehmensindividuellen Zielvorgaben, den auf langfristiger Basis am erfolgsversprechendsten Ansatz dar, denn nur diese basieren auf die organisationsspezifischen Sicherheitsbedürfnisse[76].

Die ermittelten und bewerteten Sicherheitslücken sind nun anhand eines hohen Detaillierungsgrades in Bezug möglicher Auswirkungen auf den laufenden Geschäftsbetrieb zu untersuchen. Dadurch kann sichergestellt werden, dass die späteren Lehrinhalte genauer konkretisiert und nach ihrer Intensität und Priorität bestimmt werden. Es ist sowohl aus Kostengründen als auch Akzeptanzproblemen zu verhindern, dass jedes Organisationsmitglied über sämtliche Themen der IT-Sicherheit geschult wird, da verschiedene Mitarbeiterbereiche von unterschiedlichen Sicherheitsmaßnahmen betroffen sind. Aus diesem Grund sollte eine individuelle Segmentierung in Form einer Zielgruppenanalyse vorgenommen werden[77].

Zielgruppenanalyse

Bei der Analyse der Zielgruppen bietet sich ein dreistufiges Vorgehen an[78]. Der erste Analyseschritt bildet die Auswahl der Unternehmenssegmente, die von IT-Sicherheitsmaßnahmen stark, nur bedingt oder gar nicht betroffen sind. Ist ein Unternehmenssegment von Sicherheitsmaßnahmen überhaupt nicht betroffen, können diese für die weitere Vorgehensweise ausgeschlossen werden. Für relevante Segmente wiederum können mit Hilfe einer Unterteilung in kleinere Gruppen detaillierter Sicherheitsmaßnahmen angepasst werden. Neben internen Mitarbeitern müssen bspw. auch externe Mitarbeiter, die temporär im Unternehmen tätig sind, zwingend berücksichtigt werden sodass mit Nachdruck auf die Einhaltung der Sicherheitsrichtlinien hingewiesen wird[79]. Weiter lassen sich Mitarbeitergruppen unterteilen, die innerhalb eines Unternehmens oder außerhalb der Unternehmensgrenzen tätig sind.

Die verbliebenen Zielgruppen müssen im zweiten Analyseschritt einer Bewertung unterzogen werden. Dabei lassen sich neben der Ermittlung der eigentlichen Segmentgröße, d. h. der Anzahl der Mitarbeiter innerhalb eines Segmentes, weiterhin Rückschlüsse auf das eigentliche Volumen einer Schulung ziehen. Dies erfolgt mit dem Einbezug der ermittelten Defizite im Sicherheitsbewusstsein der Zielgruppe und den daraus ermittelten Zielen der Sicherheitskampagne. Nach der Auswahl einzelner Unternehmenssegmente sowie deren Bewertung erfolgt im letzten Analyseschritt eine allgemeine Durchführbarkeitseinschätzung. Unternehmerische Kapazitäten sind begrenzt und schließen ggf. die Durchführbarkeit einer effizienten Schulung in den ermittelten Segmenten aus. Es darf nicht infolge fehlender Kapazitäten zu einer Vernachlässigung bestimmter Segmente kommen, da dies die Defizite des Sicherheitsbewuss-

[76] vgl. Schlienger (2006), S. 64
[77] vgl. Goucher (2008b), S. 15
[78] vgl. Meffert et al. (2008), S. 294
[79] vgl. Temme (2005), S. 1

tseins nicht mildern würde[80]. Vielmehr ist zu überdenken, ob weitere Kapazitäten ausgehandelt werden müssen oder ob einzelne vergleichbare Segmente zusammenzufassen sind, bei denen eine Vielzahl von Überschneidungen an zu behandelnden Themen vorliegen.

Weiterhin sind die im Rahmen der Sicherheitskultur angesprochenen Diversity-Parameter zu beachten und entsprechend auf die Zielgruppen auszulegen. Neben demografischen Merkmalen sind Erfahrungen der Mitarbeiter, Charakterzüge und Persönlichkeiten, der soziale Status und das Wertesystem eines Menschen zu berücksichtigen[81]. Diese Kenntnisse sind besonders innerhalb einer Präsenzschulung für Führungspersonen von ausschlaggebender Bedeutung. Entsprechend den jeweils ausgeprägten Parametern ist auch das Führungsverhalten entsprechend anzupassen.

4.3 Phase 3 – Design

Ein zentrales Element der Designphase ist die Ausgestaltung eines Trainings, welche, unter Berücksichtigung der Zielgruppe und vorhandenen Sicherheitslücken, die Defizite im Sicherheitsbewusstsein nahezu vollständig eliminieren sollen. Es gilt zu klären, was und mit welchen Mitteln geschult werden soll. Im Zuge der Lehrplanung ist wichtig, dass auch das Vorwissen der befragten Mitarbeiter Berücksichtigung findet. Die jeweiligen Themen sind am Entstehungspunkt zu greifen und dem Mitarbeiter vereinfacht, idealerweise anhand von Beispielen, nahe zu legen. Nur wenn die Maßnahmen auch verstanden und akzeptiert werden, kann es zu einer korrekten Interpretation der vermittelten Informationen kommen und eine daraus resultierende Verhaltensänderung bewirkt werden. Besonders für die sichtbaren Elemente einer ausgeprägten Sicherheitskultur ist es wichtig, dass diese, entsprechend dem vorhandenen Hintergrundwissen, korrekt gedeutet und interpretiert werden.

Die richtige Wahl der Lehrinhalte

Im Rahmen der Ermittlung von Lehrinhalten einer Kampagne ist grundsätzlich zwischen generellen und spezifischen Lehrinhalten zu unterscheiden. Generelle Lehrinhalte sind grundlegende Themen, wie z. B. der Umgang mit Passwörtern oder der Schutz gegenüber Social Engineering, die nahezu jede Zielgruppe betreffen. Spezifische Lerninhalte sind dagegen für eine bestimmte Zielgruppe zu konstruieren, um einen gezielteren Fokus im Rahmen eines Trainings zu erhalten. Wird bspw. ein Telearbeitsplatz betrachtet, bei der ein Mitarbeiter außerhalb der Räumlichkeiten eines Unternehmens auf das firmeninterne Netzwerk zugreift, so gilt es, diese Zielgruppe für einige Themenbereiche gesondert zu sensibilisieren.

Vorteilhaft bei der richtigen Wahl der Lehrinhalte ist, dass viele Aspekte, auch für private Zwecke eines Mitarbeiters, durchaus einen Nutzen stiften können. Sicherheitsmaßnahmen wie das sichere Anlegen eines Passwortes oder Methoden gegen Social Engineering Attacken tan-

[80] vgl. Kapitel 2.3
[81] vgl. v. Rosenstiehl et al (2003), S. 450

gieren sowohl betriebliche als auch private Interessen eines Mitarbeiters[82]. Hieraus lässt sich schließen, dass auch gezielt private Bereiche als Lehrinhalte eingesetzt werden sollten, um zu einer Förderung der intrinsischen Motivation beizutragen. Letztendlich kommt es nur dann zu einer bewussten Einhaltung der Sicherheitsmaßnahmen, wenn ein Mensch sie in Bezug auf sich selbst als wichtig erachtet[83]. Ein Mitarbeiter wird sich also vermehrt mit dem Thema der IT-Sicherheit auseinandersetzen, sofern auch eigene Interessen angetastet werden können.

Auswahl der Lernkanäle

Ein ebenso bedeutender Aspekt wie die Ermittlung der Lehrinhalte ist die Auswahl der Lernmethoden innerhalb einer Kampagne. Wie bereits angesprochen, müssen die Teilnehmenden über möglichst breit eingesetzte Kanäle angesprochen werden. *Harris et al.* analysierten in einer Studie den Einsatz verschiedener Medien auf die Effektivität von Security Awareness Trainings[84]. Sie untersuchten die Auswirkungen von hypermedia-, multimedia- und hypertextbasierten Schulungsprogrammen auf die von ihnen definierten drei Sicherheitsbewusstseinsniveaus Wahrnehmung, Verständnis und Fortschreibung[85]. Wahrnehmung bezog sich hierbei auf die Generierung eines Gefühls oder Empfindens für potenzielle Sicherheitsrisiken. Um diese korrekt bewältigen zu können, muss weiterhin ein Verständnis bzw. Hintergrundwissen, auf das konkrete Risiko bezogen, vorhanden sein. Die Fortschreibung beinhaltet die Fähigkeit der IT-Nutzer, potenzielle Risiken vorausschauend korrekt einschätzen zu können. Es konnte gezeigt werden, dass der Einsatz von multimediabasierten, im Gegensatz zu hypertextbasierten Trainingsmethoden, eine positivere Auswirkung auf das Verständnis sowie auf die Fortschreibung erzielen konnten. Dies lässt sich daraus begründen, dass textlastige, stark verschlüsselte Botschaften eine größere Aufnahme- und Verarbeitungszeit erfordern[86]. In der Wahrnehmung von IT-Risiken erwiesen sich hypertextbasierte Trainings als effektiver, so dass der Einsatz multimedialer Trainings nicht in allen Belangen als reine Trainingsmethode geeignet ist. Vielmehr kann ein derartiges Training die Aufmerksamkeit des Lernenden von den eigentlichen Lernobjekten ablenken. Dagegen bergen hypermediabasierte Trainings bergen den Vorteil, dass sie ein Grad an Anpassungsfähigkeit und Interaktivität besitzen, während reine multimediabasierte Trainings als eher starr einzustufen sind. Auf Grund dessen dominierten Hypermedia-Trainings in allen Untersuchungsbereichen die übrigen Trainingsmethoden.

Die Ergebnisse zeigen, dass der Einsatz vielfältiger Medien in einem Trainingsprogramm positive Auswirkungen auf das Lernverhalten eines Mitarbeiters hat. Dies lässt sich dadurch begründen, dass jeder Mensch verschiedene Medien zum Lernen präferiert. Informationen sind deshalb innerhalb eines Trainings auf verschiedene Weisen zu vermitteln, um möglichst jeden Mitarbeiter erreichen zu können. Hypermediabasierte Trainings sind ein probates Mittel

[82] vgl. Eurostat (2007). Laut einer Studie der Eurostats verfügten 2007 71% der Haushalte in Deutschland über einen privaten Internetzugang, bei denen es in 33% aller Fälle zu einem Datenverlust auf Grund von Viren und Trojanern gekommen ist.
[83] vgl. Anderson (2007), S. 241
[84] zu den folgenden Ausführungen vgl. Harris et al. (2008), S. 92 - 100
[85] 153 Probanden, mit etwa gleichen Sicherheitsbewusstseinsniveaus wurden dabei zufällig einem der drei Trainingsmethoden zugewiesen und mussten an einem einwöchigem Training teilnehmen.
[86] vgl. auch Dewitz/ Jürgens (2008), S. 587

zur Steigerung der Effektivität einer Security Awareness Kampagne. Besonders durch die verschiedenen Formen des E-Learnings können eine Vielzahl von Medien in die Kampagne integriert werden. Entsprechend behavioristischen Ansichten sollten einem Mitarbeiter als Reize verschiedene Informationen präsentiert werden, die darauf folgend über Software-Angebote abgefragt werden. Zeigt der Lernende das gewünschte korrekte Verhalten, so erfolgt eine Belohnung, ansonsten ist die einzelne Frage oder gar der gesamte Test zu einem späteren Zeitpunkt als „Strafmaßnahme“ zu wiederholen.

Ein weiterer wichtiger Lernkanal ist der Einsatz von Präsenzschulungen, die den Ansätzen des Kognitivismus nahekommt. Frontal werden dem Mitarbeiter die identifizierten Lehrinhalte vermittelt, wobei eine anschließende Überprüfung des vermittelten Lernstoffes mittels E-Learning Modulen erfolgen kann. Innerhalb der „Präsenzschulung“ sollte neben einfachen Präsentationen weiterhin ein besonderer Stellenwert auf die Sichtweisen der konstruktivistischen Lerntheorie gelegt werden. Da, im Gegensatz zu den übrigen Theorien, das Vorwissen eine bedeutende Rolle spielt, muss u. a. über die zuvor besprochenen Methoden ein grundlegendes Verständnis der IT-Sicherheitsmaßnahmen entwickelt werden. Erst dadurch können Informationen korrekt interpretiert werden. Nach den Ansichten der konstruktivistischen Lerntheorie ist sowohl die selbstständige Erarbeitung als auch das Erarbeiten in Lernpartnerschaften ein bedeutender Prozess zur Wissensgenerierung. Den Mitarbeitern sind dabei möglichst breite Informationen über verschiedene Lernkanäle bereitzustellen, mit denen sich die Mitarbeiter identifizieren und folglich ein Verständnis generieren können. Durch die Erarbeitung in kleineren Gruppen kann dies weiter abgerundet werden und birgt zusätzlich den Vorteil der Kommunikationsförderung und des Wissensabgleichs. Als weiteren Baustein könnten, entsprechend dem „Learning by Doing“ Ansatz, Maßnahmen eingeleitet werden, bei denen sich die Trainingsteilnehmer bspw. gegenseitig verschlüsselte E-Mails zuschicken müssen. Um die Wichtigkeit von komplexen Passwörtern zu unterstreichen, könnte die Lehrperson die Vorgehensweise eines Passwort-Finder Programms demonstrieren. Zuvor könnte ein Mitarbeiter ein einfach zu erratendes Passwort in das System eingeben, um dies anschließend mittels eines Passwort-Finders zu identifizieren.

Eine weitere Maßnahme, die den „Learning by Doing“ Ansatz mit sozialen Anreizen erweitert, stellen Rollenspiele bspw. zum Thema Social Engineering dar. Dabei könnte ein Lernpartner einen Mitarbeiter spielen und ein weiterer einen Hacker, der mittels Kommunikation versucht Benutzerdaten zu erhaschen. Dies kann sowohl vor der gesamten Gruppe als auch individuell erfolgen und ist ggf. von den Lehrpersonen weiter zu ergänzen. Auf diese Weise kann jeder einzelne Mitarbeiter ein Gefühl für derartige Angriffsmethoden entwickeln und korrektes Verhalten antizipieren. Präsentationen erweisen sich als sinnvolles Element, um bspw. Ergebnisse bestimmter Aufgaben präsentieren zu können. Diskussionen runden dabei die jeweiligen Themen weiter ab, sodass von einer reinen Betrachtung kognitivistischer Ansätze abgekehrt wird. Auch Führungskräfte sollten zu Beginn eines Trainings Präsentationen nutzen, um die Bedeutsamkeit des Sicherheitsbewusstseins weiter unterstreichen zu können.

Zu beachten ist, dass die drei Lerntheorien jeweils unter der Annahme unterschiedlicher Menschenbilder entstanden sind. Der Menschenbildtypus des „complex man“ integriert allerdings

die Annahmen sämtlicher Menschenbilder zu einem gesamten Menschenbild, so dass ausgewählte Elemente der dargestellten Lerntheorien in Abhängigkeit des in einem Unternehmen vorherrschendem Menschenbildes ausgewählt werden müssen.
Das Motivationspotenzial eines jeden Mitarbeiters wird in der Designphase im Gegensatz zur Identifikationsphase eine höhere Steigerungsrate erreichen. Besonders über die Partizipation ist in dieser Phase die intrinsische Motivation anzuregen. Eine erfolgreiche Einbindung fördert zudem die Kommunikation zwischen den Mitarbeitern und der Management-Ebene, steigert die Bereitschaft, Maßnahmen tatsächlich umzusetzen und wirkt Effizienz steigernd durch die Ideeneinbringung der Mitarbeiter. Die Partizipation hat somit neben intrinsischen Motivationseffekten, auch soziale und organisatorische Effekte, die das Motivationsniveau weiter ansteigen lassen und gleichzeitig das Unternehmensintegrationsgefühl fördert.

4.4 Phase 4 – Umsetzung

In dieser Phase geht es darum, Hintergrundwissen zu vermitteln und bereits vorhandenes Wissen aufzufrischen. Es wird davon ausgegangen, dass entsprechend den obigen Ansätzen auf die spezifizierten Zielgruppen konkretisierte, vielfältige Lehrmethoden eingesetzt werden. Sicherheitskonforme Regeln müssen derart vermittelt werden, dass die Organisationsmitglieder diese ohne großen Zusatzaufwand erlernen und verstehen können. Zu jeder Maßnahme sollten konkrete Verhaltensbeispiele passend zu jeder Zielgruppe aus der täglichen Praxis gegeben werden[87]. Auch Empfehlungen, die für den privaten Bereich Gültigkeit besitzen, erweisen sich als sinnvoll einzubeziehen. Auf diese Weise werden den Anwendern potenzielle Schadensfälle und deren mögliche Auswirkungen einfacher deutlich gemacht, was zu einem Verstärkungseffekt führen kann[88].

Weiterhin ist wichtig, dass einprägsame Elemente konstruiert und häufig wiederholt werden, um einen späteren Widererkennungseffekt erlangen zu können. Denkbar wäre der Einsatz leicht einprägsamer Slogans, die im Anschluss einer Kampagne bspw. in Form eines Posters abgedruckt werden. Diese Slogans verhelfen jedes Organisationsmitglied zur Konstruktion von Gedankenstützen, die mit einzelnen Sicherheitsmaßnahmen verbunden werden[89]. Entsprechend konstruktivistischer Prinzipien können diese Slogans von den Mitarbeitern in Lernpartnerschaften erarbeitet und ggf. mit visuellen Elementen ergänzt werden.

In Bezug auf die Motivation stellt die Umsetzung die bedeutendste Phase der Kampagne dar, da sich tief greifend Anreize integrieren lassen. Materielle Anreize sind hierbei ein sinnvoller Anknüpfungspunkt, um die Motivation der Anwender weiter zu festigen. Direkte materielle Anreize könnten bspw. in der Form einer Teilnahme an einem Preisausschreiben gemacht werden, die den Gewinn einer monetären Leistung in Aussicht stellen. Vorstellbar ist bspw. ein Preisausschreiben, bei der der beste Beitrag aus der Konstruktion des Slogans gekürt wird oder im laufenden Arbeitsprozess Verbesserungsvorschläge gemacht werden. Auch indirekte materielle Anreize, wie bspw. die Ausgabe von Essensmarken während des Trainings oder die

[87] vgl. Dewitz/ Jürgens (2008), S. 584
[88] vgl. Temme (2005), S. 2
[89] vgl. Anderson (2007), S. 261

Vergabe von sicheren USB-Sticks für den privaten Gebrauch, die wichtige Softwarelösungen wie Anti-Viren Scanner oder Verschlüsselungstools beinhalten, sind leicht integrierbar. Da besonders in der Umsetzungsphase eine Vielzahl von Anreizen eingesetzt werden, wird demnach in dieser Phase das höchste Motivationsniveau erreicht (vgl. Abbildung 4).

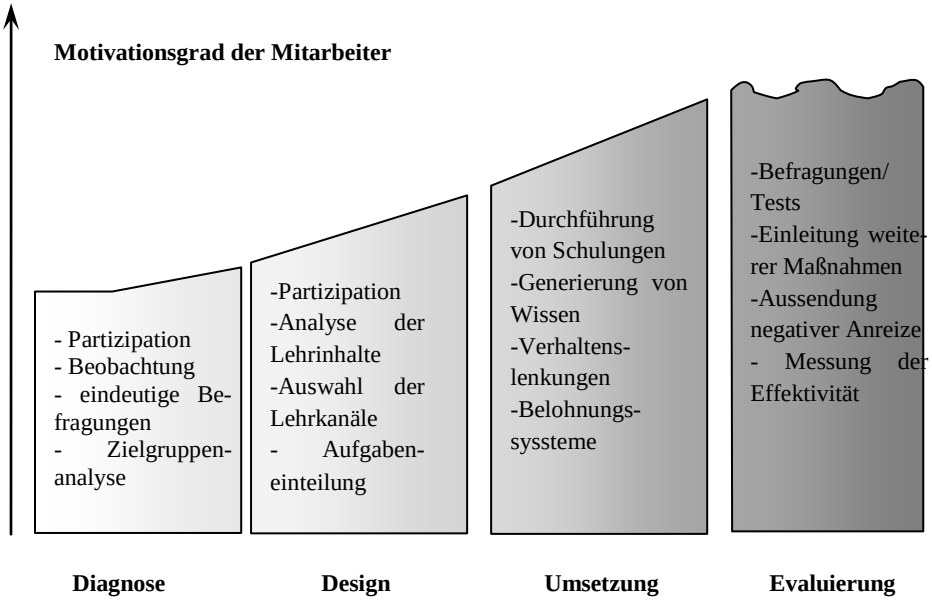


Abbildung 4 Optimale Motivationsgradentwicklung in einer Security Awareness Kampagne. Quelle: eigene Darstellung

Es wird erkennbar, dass bereits in der Diagnosephase ein geringes Motivationsniveau vorhanden ist. Dies lässt sich sowohl aus unternehmenskulturellen Hintergründen erklären, als auch, dass grundlegend, bereits aus der Arbeitstätigkeit heraus, ein Motivationsgrad vorhanden sein muss. Die Unternehmenskultur beeinflusst den Motivationsgrad auf einem bestimmten Grundniveau besonders über die Artefakte aber auch über die gelebten Werte und Normen. Zudem führt eine vorhandene Identifikation mit dem Unternehmen bereits zu einer inneren Motivation. Der Stellenwert, den die IT-Sicherheit in einem Unternehmen einnimmt, kann zwar von den Beschäftigten beobachtet werden, nur fehlt das notwendige Hintergrundwissen, für eine Bewusstseinssteuerung und wissentlichen Anwendung der Sicherheitsmaßnahmen. Mit Beginn der Designphase kann bereits, wie konkretisiert wurde, die Motivation durch Partizipation und die Wissensstandermittlung in einem geringen Maße gesteigert werden. Die Designphase profitiert ebenfalls von einer Einbindung der Mitarbeiter durch die Anregung der intrinsischen Motivation sowie sozialer Anreize. Dadurch muss es zu einer größeren Motivationssteigerung kommen als noch in der Designphase. Durch die Umsetzungsphase wird der Motivationsgrad durch die eigentliche Wissensvermittlung und die besonders vielfältig zu setzenden Anreize auf das Maximun gesteigert. In der letzten Phase, der Evaluationsphase, muss das erreichte Motivationsniveau konstant gehalten werden, wobei hier von einer Fluktuation gesprochen werden kann. Dies erklärt die Darstellung der folgenden Kapitel.

4.5 Phase 5 – Evaluierung und Verbesserung

Ist eine Umsetzung der Schulung erfolgt und den Mitarbeitern wurden die Sicherheitsmaßnahmen eingehend vermitteln, gilt es in der letzten Phase eine Evaluation durchzuführen so-

wie Maßnahmen einzuleiten, die den erreichten Motivationsgrad möglichst konstant fixieren. Die Kontrollphase zielt dabei auf die Messung der Effektivität der gesamten Sensibilisierungskampagne ab. Hierbei stellen die Durchführung von Tests unmittelbar nach der Kampagne denkbare Methoden dar, um gelehrte Wissensstände abzufragen. Ein Ansatz wäre die Durchführung einer zweiten Befragungswelle, die den Fragebogen aus der Designphase erneut aufgreift und wiederholt einsetzt. Grundlegend eignet sich für diesen Ansatz eine Panel- oder Trackingstudie. Entsprechend der Panelstudie werden vor und nach der Kampagne jeweils die gleichen Mitarbeiter befragt, was den Vorteil der Strukturgleichheit bietet. Nachteilig ist eine möglicherweise auftretende Befragungsmüdigkeit sowie das Auftreten verzerrender Lerneffekte, die sich auf Grund der ersten Befragungswellen ergeben können. In einer Trackingstudie werden bei der Befragung unterschiedliche Personen einbezogen, die allerdings von der Struktur vergleichbar sein müssen. Dadurch kann verhindert werden, dass eine Befragungsmüdigkeit sowie verzerrende Lerneffekte auftreten[90].

Auch Beobachtungen spielen in der Kontrollphase eine kennzeichnende Rolle[91]. Um die strikte Einhaltung der Sicherheitsmaßnahmen zu unterstreichen, müssen bei auftretendem Fehlverhalten negative Anreize in Form von Sanktionen oder Abmahnungen eingesetzt werden. Methoden für Kontrollmaßnahmen gibt es zahlreiche und wurden bereits in der Designphase angedeutet. Über sog. Mystery-Calls bspw. können stichprobenartig Anrufe mit dem Ziel getätigt werden, vertrauliche Unternehmensdaten von Mitarbeitern zu erlangen. Eine weitere Möglichkeit bieten Notfallübungen, die das jeweilige Verhalten in einer Gefahrensituation zeigen[92]. Beim Aussenden negativer Anreize ist ein konsequentes Verhalten empfehlenswert, da Drohungen sowie die vereinbarten Regelwerke ansonsten an Nachdruck verlieren könnten[93]. Zusätzlich wird durch konsequentes Verhalten eine Wirkung auf die übrigen Mitarbeiter erzielt, die die möglichen Sanktionen beobachten und wirkungsvoll auf das eigene Verhalten übertragen. Es ist dabei wichtig, die beschriebenen Erhebungspunkte in regelmäßigen Abständen zu wiederholen, um Veränderungen des Sicherheitsbewusstseins im Zeitverlauf frühzeitig erkennen und entsprechend reagieren zu können.

Interessante Methoden, die den Awareness-Grad nach einer Kampagne messbar machen sollen, stellen der Security Awareness Index (kurz: SAI) sowie das Effektivitätsmodell nach *Kruger* und *Kearney* dar. Beim SAI handelt es sich um ein Befragungstool, welches eine Mitarbeiterbefragung zum Sicherheitsverhalten durchführt. Die erhaltenen Antworten werden anschließend in einem Evaluationsprozess unternehmensindividuell, je nach Bedeutsamkeit des einzelnen Faktors, gewichtet. Wurden alle Fragen beantwortet und bewertet, wird daraus der Durchschnitt gebildet, der den SAI darstellt. Der höchstmögliche Wert einer Organisation ist demnach 100 und impliziert das höchste Maß an Sicherheitsbewusstsein. Mittels eines Benchmarks können anschließend die jeweiligen Schwachstellen auf einfachste Art und Weise dargestellt werden[94]. Der SAI kann sowohl vor einer Kampagne zur Ermittlung der

[90] vgl. Zerr (2007), S. 522
[91] vgl. Kap. 4.2
[92] vgl. Temme (2004), S. 13
[93] vgl. Temme (2005), S. 3
[94] zu den Ausführungen und Auswertungen des SAI vgl. Tucker (2002), S. 47 - 58

Schwachstellen, als auch nach der Kampagne zur Kontrolle und Messung der Effektivität eingesetzt werden. Bestehen trotz durchgeführter Kampagne noch Mängel im Sicherheitsbewusstsein einiger Organisationsmitglieder müssen weitere Maßnahmen ergriffen und gestaltet werden.

Das Effektivitätsmodell nach *Kruger* und *Kearney* ist dagegen komplexerer Natur[95]. Das Modell basiert, eingeteilt nach Unternehmensregionen, auf die drei Dimensionen des Wissens, der Einstellung und des Verhaltens zu entsprechenden Sicherheitsmaßnahmen. Diese werden wiederum in sechs, in der Kampagne fokussierten, Sicherheitsmaßnahmen (z. B. das Passwortverhalten) unterteilt, die des Weiteren in verschiedene Kategorien und Unterkategorien weiter aufgeteilt werden. Entsprechend den jeweilig regional unterschiedlich bedingten Anforderungen an die Sicherheitsbestimmungen, werden diese je nach Priorität mit einem Faktor vergleichbar den SAI-Ansätzen bewertet.

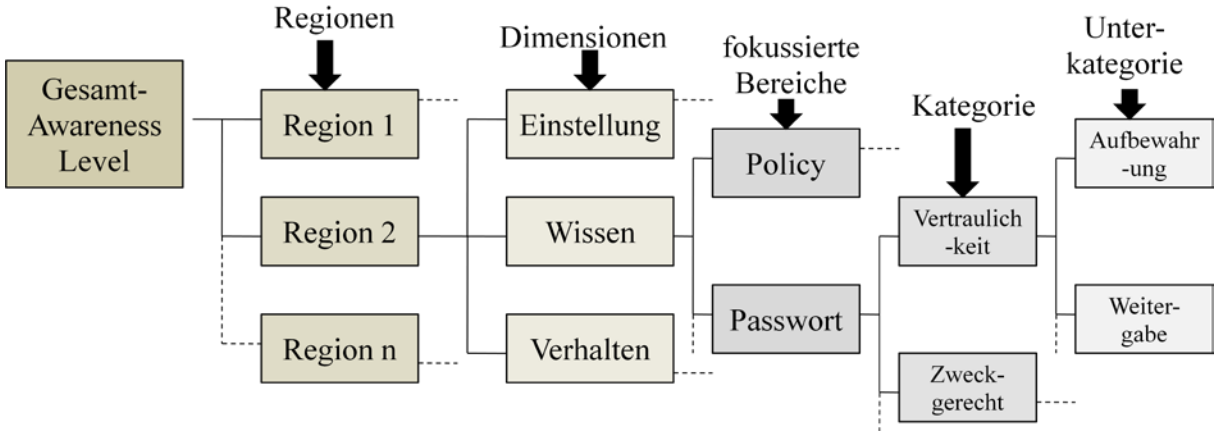


Abbildung 5 Baumdiagramm zur Vorgehensweise. Quelle: in Anlehnung an Kruger/ Kearney (2006), S. 292

Anhand der einzelnen Faktoren werden Fragen gebildet, die im Anschluss einer Kampagne von den Mitarbeitern zu beantworten sind. Die Dimension „Verhalten“ soll dabei mittels physikalischer Tests ermittelt werden. Der jeweilige Bewertungsfaktor einer Dimension wird anhand des multikriteriellen Verfahrens des analytischen Hierarchieprozesses (AHP) ermittelt, indem ein paarweiser Vergleich der verschiedenen Faktoren nach den Präferenzen des Managements vollzogen wird. Die Ergebnisse werden in einem „Regional Awareness Map“ zusammengefasst, anhand derer ersichtlich wird, wie ein spezifisches Unternehmen in der jeweiligen Dimension und dem fokussierten Bereich des Awareness Trainings agiert (vgl. Abbildung 6). Die linke Tabelle zeigt, dass der Gesamt-Awareness Grad in dem untersuchten Unternehmen bei 65% liegt. Dies kann durch die Aggregation der drei in der Horizontale ausgeprägten Dimensionen Wissen (77%), Einstellung (76%) und Verhalten (54%) ermittelt werden. Die dunkel hinterlegten Felder visualisieren, dass speziell die Verhaltenskomponente schlecht ausgeprägt ist und somit weiterer Maßnahmen bedürfen. Wird die vertikale Achse näher betrachtet, so werden jeweils die einzelnen Bereiche ersichtlich, in denen Nachholbedarf besteht. Die regelgerechte Einhaltung der IT-Sicherheitspolicy zeigt bspw. in der Dimension Einstellung (55%) und vor allem im Verhalten (18%) erhebliche Defizite, obwohl das notwendige Wissen (81%) relativ gut ausgeprägt ist. Aggregiert lässt sich hieraus wiederum ein

[95] Zu den folgenden Ausführungen vgl. Kruger/ Kearney (2006), S. 289 - 296

Ausmaß von 44% auf den „Regional Awareness Grad“ ermitteln. Diese Einteilung ermöglicht es der Führungsebene, gezielt auf die vereinzelten Defizite zu reagieren.

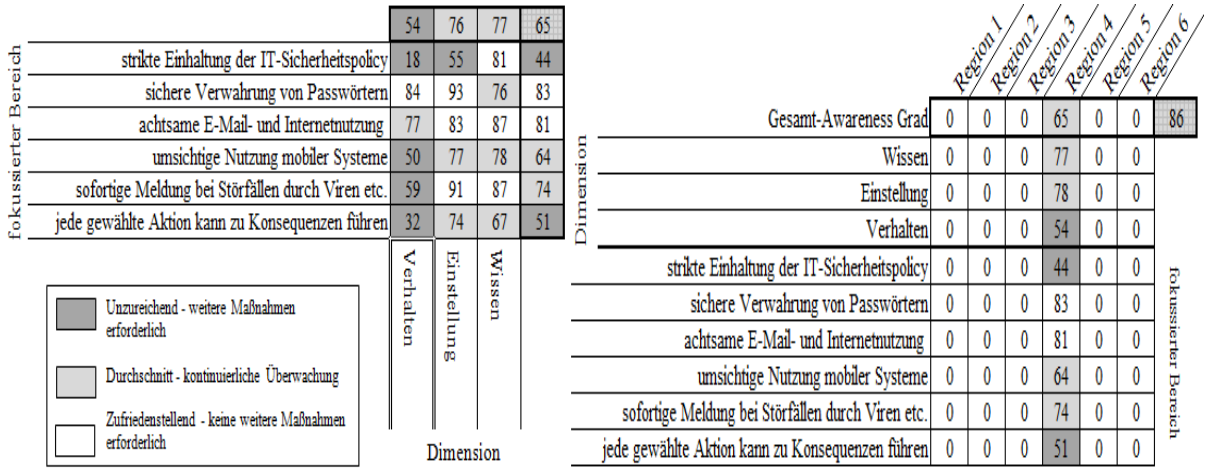


Abbildung 6 Bewertungsbogen Effektivitätsmodell. Quelle: in Anlehnung an Kruger/ Kearney (2006), S. 294

Wird nun für jedes einzelne Unternehmen eine derartige Gegenüberstellung gewählt, so lassen sich diese zu einer „Global Awareness Map“ zusammenfassen (vgl. Abbildung 6 rechte Tabelle). Illustrativ wurde hier ein „Gesamt-Awareness Grad“ von 86% ermittelt und ist als eher positiv einzustufen. Die Anwendung dieser Methode birgt den Vorteil, dass entsprechend den Bedürfnissen jedes spezifischen Unternehmens eine Bewertung vollzogen werden kann. Auch ein Awareness-Level kann numerisch ermittelt und ggf. mit anderen Unternehmensbereichen verglichen werden.

Abschließend bleibt festzuhalten, dass eine Security Awareness Kampagne nicht als einfacher Prozess angesehen werden kann. Vielmehr ist die gesamte Kampagne als ein Managementkreislauf zu verstehen, der sich stetig wiederholt. Die Erkenntnisse der Evaluationsphase fließen dann in den nächsten Prozess zur Förderung vom Sicherheitsbewusstsein ein.

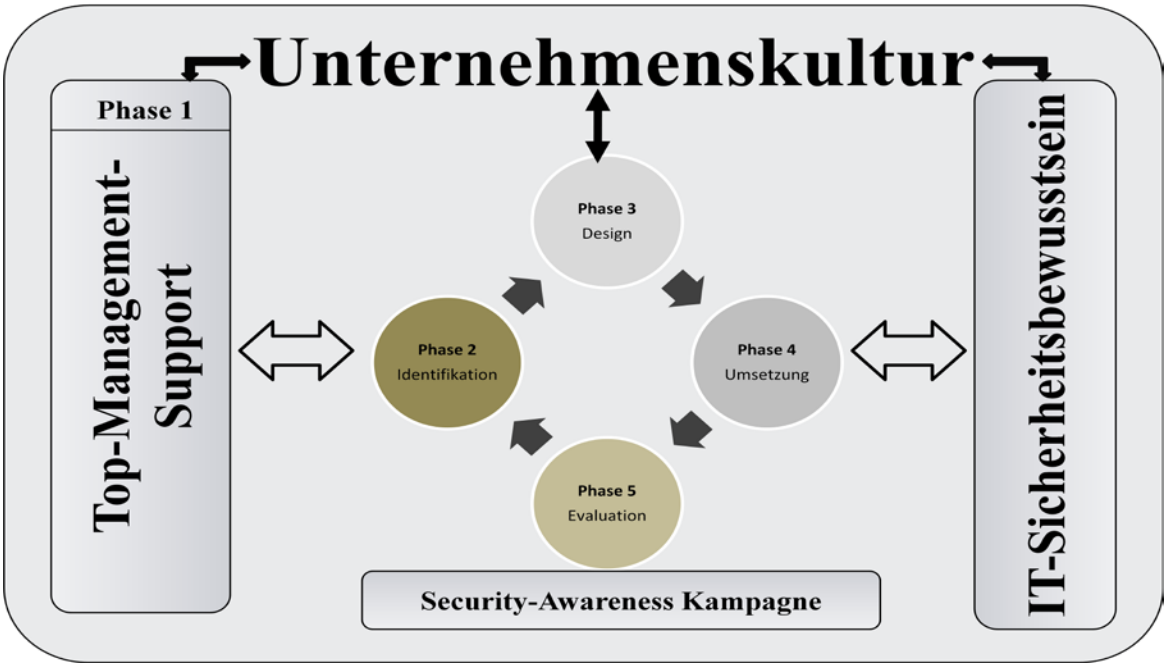


Abbildung 7 Managementkreislauf und deren Einflussfaktoren. Quelle: eigene Darstellung

Die Abbildung 7 visualisiert den Managementkreislauf über die vier Phasen der Diagnose, Design, Umsetzung und Evaluation. Dabei wirken zahlreiche Inputfaktoren, wie der Management-Support oder die Unternehmenskultur, in einem wesentlichen Maße auf die Kampagne ein. Somit muss eine starke Ausprägung dieser Elemente als Voraussetzung für eine effektive Kampagne geschaffen werden.

Damit die verschiedenen Sicherheitsmaßnahmen nicht in Vergessenheit geraten, müssen die in der Schulung entwickelten Gedankenstützen, sinnvoll in den täglichen Arbeitsprozess integriert werden. Entsprechend kognitiver Ansätze sind eine Vielzahl sensorischer Reize zu setzen, die die Wahrnehmung aktivieren und Informationen verarbeiten lassen[96]. Wird die Aufmerksamkeit des sensorischen Reizes erreicht, so kann, über die Verknüpfung erlernter Verhaltensweisen innerhalb der Kampagne auf die Informationen aus dem Langzeitgedächtnis zurückgegriffen und auf das Verhalten angepasst werden. Demzufolge sind Maßnahmen einzuleiten, welche die Thematik fest im Gedächtnis der Organisationsmitglieder verankern und die in der Phase 4 erreichte Sensibilität aufrecht halten[97]. Der Einsatz sensorischer Reize ist besonders vielfältig gestaltbar und bereits mit geringen finanziellen Mitteln zu erreichen. Die in der Umsetzungsphase zusammen mit den Mitarbeitern zusammen entwickelten Slogans, sind visuell bspw. auf Postern abzudrucken und im Unternehmen oder in einzelnen Abteilungen zu präsentieren. Auch der Einsatz von Humor ist ein interessantes Medium, um die Aufmerksamkeit kontinuierlich zu wecken und eine Bewusstseinsstärkung zu bewirken. Die visuelle Darstellung über die Gestaltung von Comics stellt bspw. eine nützliche Maßnahme dar (vgl. Abbildung 8)

Abbildung 8 Walt & Friends Cartoon. Quelle: Dewitz/ Jürgens (2008), S. 585

Weiterhin sollte den Mitarbeitern die Möglichkeit geboten werden, auf Elemente des Trainings zurückgreifen zu können. Im Falle einer Präsenzschulung könnte eine interaktive Aufzeichnung erfolgen, die im Anschluss im Intranet publiziert wird. Dadurch wird den Organisationsmitgliedern die Möglichkeit einer aktiven Nachbereitung geboten, sodass nicht verstandene oder innerhalb einer Gruppe diskutierte Inhalte erneut schnell und einfach nachvollzogen werden können. Zusätzlich sollte den Organisationsmitgliedern die Möglichkeit geboten werden, über eine öffentliche Sprechstunde oder die Einrichtung eines Forums den IT-Verantwortlichen konkrete Fragen stellen zu können[98]. Ein Forum bietet dabei den Vorteil, dass neben Fragen und Antworten zu speziellen Problemen, auch eigene Meinungen und Er-

[96] vgl. Kapitel 4.1.2
[97] vgl. Fox (2003), S. 332
[98] vgl. Temme (2005), S. 2

fahrungen Einzug finden können. Aufgetretene Probleme können dann auch von anderen Mitarbeitern eingesehen und diskutiert werden, sodass indirekt ein Qualitätszirkel gebildet wird.

Hieraus wird deutlich, dass nach einer Sensibilisierungskampagne keine Vernachlässigung des IT-Sicherheitsbewusstseins eintreten darf, in der Hoffnung ein hohes Motivationsniveau bliebe ohne weitere Maßnahmen konstant. Sobald vereinzelte Maßnahmen in Vergessenheit geraten und das Motivationsniveau zu fallen beginnt, sind gezielt Anreize zu setzen, um das Motivationsniveau erneut zu steigern. Neben Erinnerungsstützen und einer erfolgreichen Einbindung der Mitarbeiter sind auch negative Anreize ein wichtiges Element, um zu einer erneuten Steigerung der Motivation zu gelangen. Aus diesen Gründen müssen jeweils, wenn die Motivation der Anwendung der Sicherheitsmaßnahmen sinkt, neue Anreize gesetzt werden, um wiederum eine Steigerung der Motivation bewirken zu können. Dies belegt die Fluktuation des Motivationsniveaus der Abbildung 4.

5 Explorative Experteninterviews

Abschließend soll durch eine Expertenbefragung die Literatursichtung durch fachwissenschaftliche Argumentationen bestätigt und ergänzt werden.

5.1 Methodik und Gesprächspartner

Ziel der Expertenbefragung war es aus der Sicht von professionellen Beratern die theoretisch fundierten Erkenntnisse durch die deskriptive Erfassung von Tatsachen aus den Wissensbeständen der Experten zu untermauern, um die Relevanz und Bedeutung der verschiedenen Aspekte bestätigen zu können. Da der Gegenstand der Untersuchung bereits in allen Dimensionen klar umrissen wurde, sollte ein teilstrukturiertes Interview durchgeführt werden. Bei der Gestaltung der Fragen wurden offene Fragestellungen verwendet, die den Befragten eigene Antwortformulierungen ermöglichten. Die konkreten Fragestellungen wurden in Anlehnung an die theoretisch erarbeiteten Erkenntnisse ausgerichtet.

Als Experte ausgewählt wurde, wer sich durch Fachpublikationen für das Thema ausgewiesen hat oder sich auf Grund beruflicher Tätigkeit intensiv mit den Fragen der Security Awareness beschäftigt. Insgesamt konnten in einem Zeitraum vom 4. Dezember bis zum 23. Dezember 2008 zehn Probanden befragt werden.

5.2 Security Awareness aus Expertensicht – Erkenntnisse und Folgerungen

Im Folgenden sollen nun die Ergebnisse der Expertenbefragung dargestellt werden. Um einen leichten Einstieg in das Thema zu erhalten, wurde mit der Frage der Hauptquellen für fehlendes Bewusstsein bei Beschäftigten begonnen. Bereits an dieser Stelle konnten einige erstaunliche Erkenntnisse erzielt werden. Einige Experten sahen die eigentliche Quelle im Wesen des Menschen selbst. So wurden Bequemlichkeit, Selbstgefälligkeit und Autoritätsgläubigkeit als Ursprung mangelnder personeller IT-Sicherheit genannt. Weiterhin wurde auf fehlendes technisches Verständnis der Beschäftigten sowie auf eine mangelnde Identifikation mit dem Un-

ternehmen hingewiesen. Hinzu käme, dass der Gedanke einer vermeintlichen Sicherheit auf Grund von Verhaltensroutinen entstehen könnte. Auf der anderen Seite wurde die eigentliche Problematik für fehlendes Bewusstsein nicht im Wesen des Menschen gesehen, sondern im Unternehmen und den darin gelebten Werten und Normen. So wurde angedeutet, dass zunehmend die Unternehmenskulturen „zerbröseln" würden. Es gebe kaum noch klare Leitbilder und nur noch wenige Visionen innerhalb eines Unternehmens. Der Technik würde einen zunehmend höheren Stellenwert als dem Menschen zugeschrieben. Dadurch wären zu diesem Themenkomplex nicht genügend Informationen in den Unternehmen vorhanden und keine oder nur unzureichende Schulungsmaßnahmen würden durchgeführt werden. Weiter angemerkt wurde, dass häufig nur demotivierende Sicherheitsdesigns innerhalb eines Unternehmens vorherrschend wären. Zusammengefasst seien die kognitive Komponente („nicht können"), die affektive Komponente („nicht wollen") sowie das organisatorische Umfeld, das die Umsetzung sicherheitskonformen Verhaltens nicht unterstützt, die Ursprünge für fehlendes Bewusstsein. Darüber hinaus mahnten nahezu alle Probanden als Hauptquelle für fehlendes Sicherheitsbewusstsein die mangelnde Vorbildfunktion des Managements an, die somit einen bedeutenden Stellenwert im Bereich Security Awareness einnimmt. Der Mensch orientiert sich in starkem Maße an eine Gruppe und passt das eigene Verhalten stark an das unmittelbare und mittelbare Umfeld an, welches wiederum die eigentliche Sicherheitskultur prägt.

Als nächsten Punkt wurden in der Praxis häufig eingesetzte Methoden zur Identifikation von Sicherheitslücken hinterfragt. Die Selbsteinschätzungsmethode der IT-Abteilung (6)[99] als erste Intention für eine Kampagne werden neben Mitarbeiterfragebögen (5) in der Praxis am häufigsten verwendet, um Sicherheitslücken beim Menschen identifizieren zu können. Beobachtungen (3) werden wiederum eher mit Vorsicht betrachtet, da diese auch zu Missverständnissen auf der Mitarbeiterebene führen können und der Eindruck einer totalen Überwachung entstehen könnte. Einzelinterviews werden als kostspieliges Spektrum eher selten angewandt (1). Als weitere mögliche Methoden wurden darüber hinaus Audits (2), aktive Tests z. B. im Bereich Social Engineering (1) sowie das „Bauchgefühl der Security Experten" genannt (1).

Nach den Befragungsmethoden wurde der präferierte Einsatz von Lehrmethoden in der Praxis hinterfragt. Auffällig bei den Ergebnissen war, dass in keinem Fall reine Präsentationen als alleinige Maßnahme zur Mitarbeitersensibilisierung genannt wurden. Präsentationen wurden nur in Kombination mit direkt am Arbeitsplatz durchzuführenden Web-based Trainings oder mittels E-Learning Modulen genannt (sog. blended learning).
Wichtig sei vor allem die Praxisnähe sowie das Aufzeigen von Konsequenzen, Lösungen und Maßnahmen. Reine Präsentationen sind bekanntlich eine Methode kognitiver Ansätze, sodass die getroffenen Annahmen einer Verknüpfung der Lehrparadigmen in einer Awareness Kampagne bestätigt werden konnten. Als weitere interessante Lehrmethoden wurden Live-Hacking Veranstaltungen genannt, bei denen bspw. den Schulungsteilnehmern die Funktionsweisen von Passwort-Finder erläutert werden.

[99] Die Zahl in Klammern zeigt die jeweilige Stimmenanzahl an.

Besonders hervorzuheben innerhalb eines Trainings sei primär die aktive Einbindung der Mitarbeiter in möglichst realitätsnahe Vorgänge. Dies spricht einen Awareness-Ansatz an, der den Kontakt an sich in den Mittelpunkt stellt. Trainings und Kommunikationstools würden dabei die Grundlage für prozess-orientiertes Awareness bilden. Am Wichtigsten sei es, dass sich das Thema Sicherheit zu einem Dauerbrenner im Unternehmen etablieren würde. Richtige Werbemaßnahmen würden somit die Auseinandersetzung mit Sicherheitsthemen unter den Mitarbeitern fördern und folglich die Awareness in einem Unternehmen steigern. Sämtliche Punkte weisen somit auf die bereits in der Arbeit eingegangene zielgruppenspezifische Wissensvermittlung mit einem zielgruppengerechten Methoden- und Medienmix hin, um auf die Individualität jedes Mitarbeiters eingehen zu können[100].

Bei der Frage der Effektivitätsmessung nach der Durchführung einer Awareness Kampagne bestand großenteils Einigkeit, dass ein reines Abfragen erlernten Wissens nicht erfolgsversprechend sei, da Bewusstsein nicht einfach messbar wäre. Vielmehr seien die Beteiligten z. B. im Rahmen von Face-to-Face Interviews zu befragen, was sich durch die Kampagne wirklich verändert hätte. Allen voran wurde der Aspekt der Beobachtung genannt, indem Statistiken über Supportanfragen interner Sicherheitsvorfälle oder den Verlust von mobilen Endgeräten ausgewertet werden würden. Überdies könne über Security Audits bspw. Social Engineering Attacken simuliert werden. Allerdings seien Wissensabfragen über ex ante – ex post Befragungen in der Praxis weit verbreitet. Angemerkt wurde allerdings häufig, dass nur selten die wirkliche Effektivität gemessen werden würde, da meist erhebliche Budgetprobleme bei der Umsetzung von Kampagnen vorhanden seien. Resümierend zeigte sich, dass in der Praxis häufig Erfolgsmessungen mittels vorher-nachher Befragungen durchgeführt werden. Eine konkrete Erfassung des Verhaltens nach einer Kampagne wird dabei vielfach vernachlässigt. Auch die Wichtigkeit einer Erfolgsmessung, um verbliebene Sicherheitslücken identifizieren und darauf reagieren zu können, wird häufig unterschätzt. Die Effektivität der gesamten Kampagne sei dadurch in Frage gestellt.

Nächster Kernpunkt der Befragung lag auf die Bedeutsamkeit des Management-Supports. Neun der befragten Experten kritisierten klar, dass der Stellenwert der Informationssicherheit vom Top-Management häufig unterschätzt werden würde. Deutlich darauf hingewiesen wurde von jedem Probanden, dass Führungspersonen als Vorbildfunktionen einen wesentlichen Teil innerhalb einer Awareness Kampagne bilden würden. Nicht ausreichend sei die Bereitschaft lediglich als „Sponsor“ aufzutreten. Vielmehr sei eine aktive Mitwirkung und das Vorleben von Sicherheitsmaßnahmen Voraussetzung, um den normativen Rahmen festzusetzen, ohne den eine Kampagne wenig wertvoll sei. Führungskräfte kämen somit speziellen Aufgaben zu. Als Multiplikatoren und Vorbilder müssten die ihnen zugeordneten Mitarbeiter von der Wichtig- und Richtigkeit des Verhaltens überzeugt werden. Wiederholt sei deutlich zu machen, dass entsprechende Initiativen auch bei Widerstand unterstützt würden. In diesem Zusammenhang sei es bedeutend, dass auch unangenehme Weisungen „durchgedrückt“ werden würden.

[100] vgl. Kap. 4.3

Neben einem unzureichenden Management-Support wurden weitere zahlreiche Risiken genannt, die sich im Zuge der Umsetzung einer Kampagne ereignen könnten. Problematisch seien meist unrealistische Erwartungshaltungen und Unkenntnis methodischer Grundlagen zur nachhaltigen Veränderung menschlichen Verhaltens. Nachhaltigkeit könne nicht durch eine Einmalaktion oder durch ein Produkt von der Stange erreicht werden. Überdies bestünde das Problem, dass Lehrthemen nicht attraktiv „verpackt“ oder zu viele Themen gewählt werden würden, die den Mitarbeiter mit Informationen förmlich erschlagen. Das Thema IT-Sicherheit müsse vermarktet werden, sodass auch die Wahl des richtigen Coaches zur Wissensvermittlung durchaus auch ein Risiko darstellen könne. Positives und richtiges Verhalten dürfe auch Spaß machen und nicht jede Vorschrift sei mit Drohgebärden zu vermitteln, sondern vielmehr mit Überzeugung. Wer Mitarbeiter durch zu restriktive Vorschriften eher an der Arbeit hindert als diese zu fördern, dürfe sich auch über Fehlverhalten dieser nicht wundern. Auch eine mangelnde Interdisziplinarität z. B. zum Human Ressource Bereichs oder allgemein die Einbindung interner Kommunikationswege stelle ein großes Problem dar. Besonders problematisch sei es, für mehr Sicherheit zu werben, während durch Entlassungen soziale Sicherungen gekappt werden würden.

Mit der letzten offenen Teilfrage wurde hinterfragt, inwieweit Sicherheitsmaßnahmen Einschnitte in die Unternehmenskultur bedeuten könnten. Hierbei sei besonders wichtig, Misstrauen und das Nicht-Zugänglich-Machen von Informationen durch ein positives Klima des Vertrauens und der Offenheit abzulösen. Einschnitte im Sinne von aggressiver Kulturänderung seien dann nötig, wenn Notfall-Maßnahmen umgesetzt und stark sicherheitsgefährdendes Verhalten abrupt gestoppt werden müsste. Demzufolge können Einschnitte tatsächlich zu einem Umdenken und zu einer Kulturänderung bzgl. des Wertedenkens führen. Im Idealfall solle es aber mehr eine Evolution denn ein Einschnitt darstellen, denn gute Awareness-Kampagnen seien auch immer Leitbild-Kampagnen, welche die Sicherheit als wichtiges Unternehmensasset betonen würden. Sicherheitsbewusstsein sei bereits zu einem gewissen Maß in der Unternehmenskultur verankert, sodass sich diese gegenseitig ergänzen und mitprägen würden. Abschließend sei zusammenzufassen, dass sich diejenigen, die Security Awareness erfolgreich umsetzen wollen, auch damit befassen müssen, um die jeweiligen Konsequenzen dies für die Unternehmenskultur abschätzen zu können. Dies sei allerdings nicht nur eine Frage der Einschnitte. Die erhaltenen Antworten stimmten den Annahmen der Unternehmenskultur eindeutig zu. Sicherheitsfördernde Maßnahmen können durchaus Einschnitte in die Unternehmenskultur bedeuten, wobei natürlich die Betonung auf eine gegenseitige Beeinflussung liegen sollte.

6 Fazit

Dem Faktor Mensch wird innerhalb einer Organisation im Rahmen des Risikomanagements ein bedeutender Stellenwert zugeschrieben. Um Informationen, Daten oder schutzwürdige Belange nachhaltig schützen zu können, steht das Risikomanagement vor der umfassenden Aufgabe, die Gefahr, die von den eigenen Mitarbeitern ausgeht, zu identifizieren und anschließend Handlungsbedarf aufzuzeigen. Die Konstruktion einer Security Awareness Kampagne ist oft ein probates Mittel zur Internalisierung des Faktors Mensch in der IT-Sicherheit

mit dem Ziel der Steigerung des Sicherheitsbewusstseins. Das Thema Mensch zeugt in einer umfassenden Security Awareness Kampagne von hoher Komplexität und Interdisziplinarität. Menschen in Organisationen sind komplexe Wesen, die durch verschiedene Persönlichkeiten, Fähigkeiten und Motive geprägt werden („complex man“). Es gibt keine allgemeine Führungsstrategie, weshalb, vor allem im äußerst sensiblen Bereich der Informationssicherheit, eine möglichst hohe Bandbreite von Anreizen in eine Kampagne integriert werden müssen, um möglichst jeden Mitarbeiter von der Relevanz und der tatsächlichen Umsetzung der Sicherheitsmaßnahmen überzeugen und motivieren zu können. Neben der Verhaltenskomponente ist überdies die Einstellungskomponente gegenüber IT-Sicherheitsmaßnahmen gezielt zu fördern. Hierbei sind ausgewählte Ansätze der drei großen Lerntheorien des Behaviorismus, Kognitivismus und Konstruktivismus einzubeziehen, um eine zielgerichtete Wissensgenerierung erreichen und optimale Umsetzung gewährleisten zu können. Eine umfassende, strategisch ausgerichtete Security Awareness Kampagne ist grundlegend in fünf Phasen zu unterteilen. Diese bestehen aus einer Grundphase, in der eine Identifikation und Förderung der IT-Sicherheitskultur vollzogen und die Steigerung des Management-Supports erreicht werden soll, einer Diagnose-, Design-, Umsetzungs- und Evaluierungsphase. In jeder Phase ist anhand der eingesetzten pädagogischen Elemente und entsprechend den Annahmen des Menschenbildes eine Vielzahl von Anreizen einzusetzen. Nur dadurch ist es möglich, das Motivationsniveau über die Phasen kontinuierlich zu steigern und entsprechend Nachhaltigkeit zu erzeugen. Bedeutend ist, dass mit der Evaluierungsphase ein durchgehender Verbesserungsprozess eingesetzt wird, um auch nach der Kampagne das Sicherheitsbewusstsein auf einem hohen Niveau fixieren zu können. Der Stellenwert von Sicherheitsbewusstsein innerhalb von Unternehmen wird somit vor allem in den nächsten Jahren weiter an Aktualität gewinnen und sich durch weitere interdisziplinäre Ansätze auszeichnen müssen, um den Faktor Mensch internalisieren zu können.

7 Literaturverzeichnis

<kes>/ Mircrosoft (2008): <kes>/ Microsoft: Lagebericht zur Informationssicherheit (1). In: <kes> - Zeitschrift für Kommunikations- und EDV Sicherheit. Ausgabe 4/2008, S. 18 - 25

Anderson/ Funke (2007): Anderson, J., Funke, J. (Hrsg.): Kognitive Psychologie – Deutsche Ausgabe. 6. Auflage, Springer Verlag, Berlin 2007

Baitsch (1999): Baitsch, C.: Interorganisationale Lehr- und Lernnetzwerke. In: Arbeitsgemeinschaft Qualifikations-Entwicklungs-Management (Hrsg.): Kompetenzentwicklung ´99. Waxmann Verlag, Münster 1999

Becher (1990): Becker, F.: Anreizsysteme für Führungskräfte. Poeschel, Stuttgart 1990

Becker (2008): Becker, M.: Messung und Bewertung von Humanressourcen. Schäffer-Poeschel Verlag, Stuttgart 2008

Breitner/ Pomes (2005): Breitner, M., Pomes, R.: IT-Sicherheit – Kein Selbstzweck sondern Notwendigkeit. In: IZN Mail Ausgabe 4 Oktober 2005

Dewitz/ Jürgens (2008): Dewitz, A., Jürgens, P.: Zu viele Regeln im Sicherheitskonzept?. In: Datenschutz und Datensicherheit, Ausgabe 9/2008

Eurostat (2007): Eurostat: Einzelpersonen mit Internet-Zugang, bei denen Sicherheitsprobleme aufgetreten sind. URL: http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do?tab=table&plugin=1&init=1&pcode=tin00069&language=de, Abgerufen am 17. November 2008, 15:51 Uhr, 2007

Fox (2003): Fox, D.: Security Awareness – Die Wiederentdeckung des Menschen in der IT-Sicherheit. In: Datenschutz und Datensicherheit (DuD), Bd. 27, 2003

Fox/ Kaun (2005): Fox, D., Kaun, S.: Security Awareness Kampagnen. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheit geht alle an!, Tagungsband zum 9. Deutschen IT-Sicherheitskongress. Gau-Algesheim, 2005, S. 329 – 337

Goucher (2008a): Goucher, W.: Enabling secure behavior. In: Computer Fraud & Security. Volume 2008, Issue 2, Februar 2008, S. 12 – 14

Goucher (2008b): Goucher, W.: Getting the most from training sessions: the art of raising security awareness without curing insomnia. In: Computer Fraud & Security. Volume 2008, Issue 4, April 2008, S. 15

Gurtner et al. (2007): Gurtner, H., Habermayr, J., Schmid, B.: Mentoring bei der schweizerischen Post – Erfahrene Führungskräfte als Türöffner für den Kadernachwuchs. In: Thom, N., Zaugg, R. (Hrsg.): Moderne Personalentwicklung. GWV Fachverlage, Wiesbaden 2007

Harris et al. (2008): Harris, A., Shaw, R., Chen, C., Huang, H.: The impact of information richness on information security awareness. In: Computers & Education, Volume 52, Issue 1, January 2008, S. 92 – 100

Helisch (2007): Helisch, M.: Einflüsse auf das sicherheitsbezogene Verhalten – Awareness-Arbeit und Unternehmenskultur. In: LANLine Ausgabe Spezial4/2007, S. 11 – 15

Helisch (2008): Helisch, M.: Security Awareness aus werbepsychologischer Sicht. Security-Manager.de – Das IT-Security Portal, URL:

http://www.securitymanager.de/magazin/artikel_1740_security_awareness_aus_werbepsychologischer.html, Abruf am 26. Oktober 2008, 10:40 Uhr

Hentze et al. (2005): Hentze, J., Graf, A., Kammel, A., Lindert, K.: Personalführungslehre. 4. Auflage, Haupt Verlag, Berlin 2005

Hofstede (2001): Hofstede, G.: Culture´s Consequences: Comparing values, behaviors, institutions and organizations across nations. 2nd Edition, Sage Publications, London/ New Dehli 2001

Jahner/ Krcmar (2006): Jahner, S., Krcmar, H.: Risikokultur als zentraler Erfolgsfaktor für ein ganzheitliches IT- Risk Management. URL: http://www.winfobase.de/lehrstuhl/publikat.nsf/intern01/8767E03F1AEBB920C12570D1003996D4/$FILE/05-38.pdf, Abruf am 3. November 2008, 10:57 Uhr

Kerres (2001): Kerres, M.: Multimediale und telemediale Lernumgebungen. Oldenbourg Wissenschaftsverlag, München 2001

Kirchler et al. (2008): Kirchler, E., Meier-Pesti, K., Hofmann, E.: Menschenbilder. In: Kirchler, E. (Hrsg.): Arbeits- und Organisationspsychologie. 2. Auflage, Facultas Verlags- und Buchhandels AG, Wien 2008

Knapp/ Marshall (2007): Knapp, K., Marshall, T.: Top Management support essential for effective information. In: Tipton, H., Krause, M.: Information Security Management Handbook. 6. Edition, Auerbach Publications, Boca Raton/ New York, 2007

Krapp/ Weidemann (2006): Krapp, A., Weidemann, B.: Pädagogische Psychologie. 5. Auflage, Beltz Verlag, Weinheim/ Basel, 2006

Kruger/ Kearney (2006): Kruger, H., Kearney, W.: A prototype for assessing information security awareness. In: Computer & Security, Vol. 25, 2006, S. 289 – 296

Lenz (2007): Lenz, R.: Sensibilität erzeugen, Bewusstsein bilden. In: Sicherheitsingenieur, Ausgabe 9/ 2007, S. 26 – 30

Meffert et al. (2008): Meffert, H., Burmann, C., Kirchgeorg, M.: Marketing – Grundlagen marktorientierter Unternehmensführung. 10. Auflage, GWV Fachverlage, Wiesbaden 2008

Mietzel (2007): Mietzel, G.: Pädagogische Psychologie des Lernens und Lehrens. 8. Auflage, Hogrefe, Göttingen, 2007

Pokoyski (2006): Pokoyski, D.: Entsicherung am Arbeitsplatz – Studie entschlüsselt erstmalig psychologische Wirkweise und Zusammenhänge der IT-Security. In: Kes. Band 6/2006, S. 61 – 62

Reinmann (2005): Reinmann, G.: Blended Learning in der Lehrerbildung. Pabst Science Publishers, Lengerich 2005

Riley (2006): Riley, S.: Password Security: What users know and what they actually do. In: Usability News, Vol. 8 Issue 1, February 2006, URL: http://psychology.wichita.edu/surl/usabilitynews/81/pdf/Usability%20News%2081%20-%20Riley.pdf, Abruf am 23. Oktober 2008, 08:55 Uhr

v. Rosenstiehl (2003): Rosenstiehl, L. von , Regnet, E., Domsch, M.: Führung von Mitarbeitern. 5. Auflage, Schäffer-Poeschel Verlag, Stuttgart 2003

von der Ruhr/ Bosse (2006): Ruhr, J. von der, Bosse, N.: Job Rotation und Job Families. In: Bröckermann, R., Müller-Vorbrüggen, M. (Hrsg.): Handbuch Personalentwicklung. Schäffer-Poeschel Verlag, 2006

Röll (2003): Röll, F.: Pädagogik der Navigation. Kopaed, München 2003

Santa (2007): Santa, I.: Das Management für Awareness begeistern. In: LanLine, Ausgabe Juli 2007, URL: http://www.lanline.de/articles/das_management_fuer_awareness_begeistern:/2007007/31141890_ha_LL.html?thes=8001,9786,10191, Abruf 25. Oktober 2008, 13:41

Schlienger (2008): Schlienger, T.: Informationssicherheit mit Kultur. URL: http://www.securitymanager.de/magazin/artikel_891_informationssicherheit_mit_kultur.html, Abruf am 24.10.2008, 18:40

Schmidt (2006): Schmidt, K.: Der IT-Security Manager. Carl Hanser Verlag, München/ Wien 2006

Scholz (1994): Scholz, C.: Personalmanagement – Informationsorientierte und verhaltenstheoretische Grundlagen. 4. Auflage, Vahlen, München 1994

Schumacher (2008): Schumacher, T.: Wo die IT-Risiken lauern. In: Computerwoche 34 (2008), S. 16-17

Siebert (2005): Siebert, H.: Pädagogischer Konstruktivismus. 3. Auflage, Beltz Verlag, Weinheim/ Basel 2005

Skinner (1982): Skinner, B.-F.: Wissenschaft und menschliches Verhalten. Kindler, München 1982

Staehle (1999): Staehle, W.: Management. 8. Auflage, Verlag Franz Vahlen, München 1999

Stuber (2002): Stuber, M.: Diversity als Strategie. In: Personalwirtschaftslehre, Ausgabe 1/2002, S. 28 – 33

Temme (2004): Temme, M.: (Un)-Sicherheitspotenzial Mitarbeiter. In: <kes> – Zeitschrift für Kommunikations- und EDV-Sicherheit. Ausgabe 2/2004, S. 10 -14, 2004

Temme (2004): Temme, M.: (Un)-Sicherheitspotenzial Mitarbeiter. In: <kes> – Zeitschrift für Kommunikations- und EDV-Sicherheit. Ausgabe 2/2004, S. 10 -14, 2004

Temme (2005): Temme, M.: Personelle IT-Sicherheit – Mehr als nur awareness. In: IT-Security 2/2005, S. 1 – 3. URL: http://www.btp-consulting.de/downloads/itsec_ch_05.pdf, Abruf am 11. November 2008, 9:22 Uhr

Tucker (2002): Tucker, T.: Security Awareness Index Report: The state of security Awareness among organizations worldwide. URL: http://security.ittoolbox.com/pub/AM101502a.pdf, Abgerufen am 13. September 2008, 10:41 Uhr

Weinberg (1999): Weinberg, J.: Lernkultur – Begriff, Geschichte, Perspektive. In: Arbeitsgemeinschaft Qualifikations-Entwicklungs-Management (Hrsg.): Kompetenzentwicklung ´99. Waxmann Verlag, Münster 1999

Weinert (1998): Weinert, A.: Organisationspsychologie. 4. Auflage, Psychologie Verlags Union, Weinheim 1998

Wirtz/ Sammerl (2003): Wirtz, B., Sammerl, N.: Innovationen in der Internet-Ökonomie. In: Habann, F. (Hrsg.): Innovationsmanagement in Medienunternehmen. Gabler Verlag, Wiesbaden, 2003

Zerr (2006): Zerr, K.: Befragung hilft beim Bewusstseins-Check. In: Computer-Zeitung, Ausgabe 36/2006, S. 23

Zerr (2007): Zerr, K.: Security-Awareness-Monitoring – Ein soziowissenschaftlicher Ansatz zur Messung des Sicherheitsbewusstseins bei Mitarbeitern. In: Datenschutz und Datensicherheit, Ausgabe 7/2007, S. 519 – 523

Zinzius (2006): Zinzius, B.: China Business – Der Ratgeber zur erfolgreichen Unternehmensführung im Reich der Mitte. 2. Auflage, Springer-Verlag, Berlin/ Heidelberg, 2006

IWI Discussion Paper Series/Diskussionsbeiträge

ISSN 1612-3646

Michael H. Breitner, *Rufus Philip Isaacs and the Early Years of Differential Games*, 36 p., #1, January 22, 2003.

Gabriela Hoppe and Michael H. Breitner, *Classification and Sustainability Analysis of e-Learning Applications*, 26 p., #2, February 13, 2003.

Tobias Brüggemann und Michael H. Breitner, *Preisvergleichsdienste: Alternative Konzepte und Geschäftsmodelle*, 22 S., #3, 14. Februar, 2003.

Patrick Bartels and Michael H. Breitner, *Automatic Extraction of Derivative Prices from Webpages using a Software Agent,* 32 p., #4, May 20, 2003.

Michael H. Breitner and Oliver Kubertin, *WARRANT-PRO-2: A GUI-Software for Easy Evaluation, Design and Visualization of European Double-Barrier Options,* 35 p., #5, September 12, 2003.

Dorothée Bott, Gabriela Hoppe und Michael H. Breitner, *Nutzenanalyse im Rahmen der Evaluation von E-Learning Szenarien*, 14 S., #6, 21. Oktober, 2003.

Gabriela Hoppe and Michael H. Breitner, *Sustainable Business Models for E-Learning*, 20 p., #7, January 5, 2004.

Heiko Genath, Tobias Brüggemann und Michael H. Breitner, *Preisvergleichsdienste im internationalen Vergleich*, 40 S., #8, 21. Juni, 2004.

Dennis Bode und Michael H. Breitner, *Neues digitales BOS-Netz für Deutschland: Analyse der Probleme und mögliche Betriebskonzepte,* 21 S., #9, 5. Juli, 2004.

Caroline Neufert und Michael H. Breitner, *Mit Zertifizierungen in eine sicherere Informationsgesellschaft*, 19 S., #10, 5. Juli, 2004.

Marcel Heese, Günter Wohlers and Michael H. Breitner, *Privacy Protection against RFID Spying: Challenges and Countermeasures*, 22 p., #11, July 5, 2004.

Liina Stotz, Gabriela Hoppe und Michael H. Breitner, *Interaktives Mobile(M)-Learning auf kleinen End-geräten wie PDAs und Smartphones*, 31 S., #12, 18. August, 2004.

Frank Köller und Michael H. Breitner, *Optimierung von Warteschlangensystemen in Call Centern auf Basis von Kennzahlenapproximationen,* 24 S., #13, 10. Januar, 2005.

Phillip Maske, Patrick Bartels and Michael H. Breitner, *Interactive M(obile)-Learning with UbiLearn 0.2*, 21 p., #14, April 20, 2005.

Robert Pomes and Michael H. Breitner, *Strategic Management of Information Security in State-run Organizations,* 18 p., #15, May 5, 2005.

Simon König, Frank Köller and Michael H. Breitner, *FAUN 1.1 User Manual,* 134 p., #16, August 4, 2005.

Christian von Spreckelsen, Patrick Bartels und Michael H. Breitner, *Geschäftsprozessorientierte Analyse und Bewertung der Potentiale des Nomadic Computing,* 38 S., #17, 14. Dezember, 2006.

Stefan Hoyer, Robert Pomes, Günter Wohlers und Michael H. Breitner, *Kritische Erfolgsfaktoren für ein Computer Emergency Response Team (CERT) am Beispiel CERT-Niedersachsen,* 56 S., #18, 14. Dezember, 2006.

Christian Zietz, Karsten Sohns und Michael H. Breitner, *Konvergenz von Lern-, Wissens- und Personalmanagementssystemen: Anforderungen an Instrumente für integrierte Systeme,* 15 S., #19, 14. Dezember, 2006.

Christian Zietz und Michael H. Breitner, *Expertenbefragung „Portalbasiertes Wissensmanagement": Ausgewählte Ergebnisse*, 30 S., #20, 5. Februar, 2008.

IWI Discussion Paper Series/Diskussionsbeiträge

ISSN 1612-3646

Harald Schömburg und Michael H. Breitner, *Elektronische Rechnungsstellung: Prozesse, Einsparpotentiale und kritische Erfolgsfaktoren*, 36 S., #21, 5. Februar, 2008.

Halyna Zakhariya, Frank Köller und Michael H. Breitner, *Personaleinsatzplanung im Echtzeitbetrieb in Call Centern mit Künstlichen Neuronalen Netzen*, 35 S., #22, 5. Februar, 2008.

Jörg Uffen, Robert Pomes, Claudia M. König und Michael H. Breitner, *Entwicklung von Security Awareness Konzepten unter Berücksichtigung ausgewählter Menschenbilder*, 14 S., #23, 5. Mai, 2008.

Johanna Mählmann, Michael H. Breitner und Klaus-Werner Hartmann, *Konzept eines Centers der Informationslogistik im Kontext der Industrialisierung von Finanzdienstleistungen*, 19 S., #24, 5. Mai, 2008.

Jon Sprenger, Christian Zietz und Michael H. Breitner, *Kritische Erfolgsfaktoren für die Einführung und Nutzung von Portalen zum Wissensmanagement*, 44 S., #25, 20. August, 2008.

Finn Breuer und Michael H. Breitner, *„Aufzeichnung und Podcasting akademischer Veranstaltungen in der Region D-A-CH": Ausgewählte Ergebnisse und Benchmark einer Expertenbefragung*, 30 S., #26, 21. August, 2008.

Harald Schömburg, Gerrit Hoppen und Michael H. Breitner, *Expertenbefragung zur Rechnungseingangsbearbeitung: Status quo und Akzeptanz der elektronischen Rechnung*, 40 S., #27, 15. Oktober, 2008.

Hans-Jörg von Mettenheim, Matthias Paul und Michael H. Breitner, *Akzeptanz von Sicherheitsmaßnahmen: Modellierung, Numerische Simulation und Optimierung,* 30 S., #28, 16. Oktober, 2008.

Markus Neumann, Bernd Hohler und Michael H. Breitner, *Bestimmung der IT-Effektivität und IT-Effizienz serviceorientierten IT-Managements,* 20 S., #29, 30. November, 2008.

Matthias Kehlenbeck und Michael H. Breitner, *Strukturierte Literaturrecherche und -klassifizierung zu den Forschungsgebieten Business Intelligence und Data Warehousing,* 10 S., #30, 19. Dezember, 2009.

Michael H. Breitner, Matthias Kehlenbeck, Marc Klages, Harald Schömburg, Jon Sprenger, Jos Töller und Halyna Zakhariya, *Aspekte der Wirtschaftsinformatikforschung 2008,* 128 S., #31, 12. Februar, 2009.

Sebastian Schmidt, Hans-Jörg v. Mettenheim und Michael H. Breitner, *Entwicklung des Hannoveraner Referenzmodels für Sicherheit und Evaluation an Fallbeispielen,* 30 S., #32, 18. Februar, 2009.

Sissi Eklu-Natey, Karsten Sohns und Michael H. Breitner, *Buildung-up Human Capital in Senegal - E-Learning for School drop-outs, Possibilities of Lifelong Learning Vision,* 39 S., #33, July 1, 2009.

Horst-Oliver Hofmann, Hans-Jörg von Mettenheim und Michael H. Breitner, *Prognose und Handel von Derivaten auf Strom mit Künstlichen Neuronalen Netzen,* 34 S., #34, 11. September, 2009.

Christoph Polus, Hans-Jörg von Mettenheim und Michael H. Breitner, *Prognose und Handel von Öl-Future-Spreads durch Multi-Layer-Perceptrons und High-Order-Neuronalnetze mit Faun 1.1 ,* 55 S., #35, 18. September, 2009.