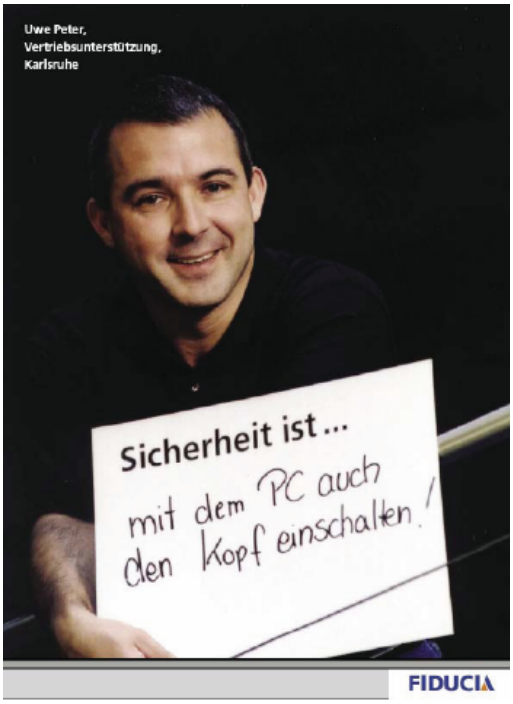
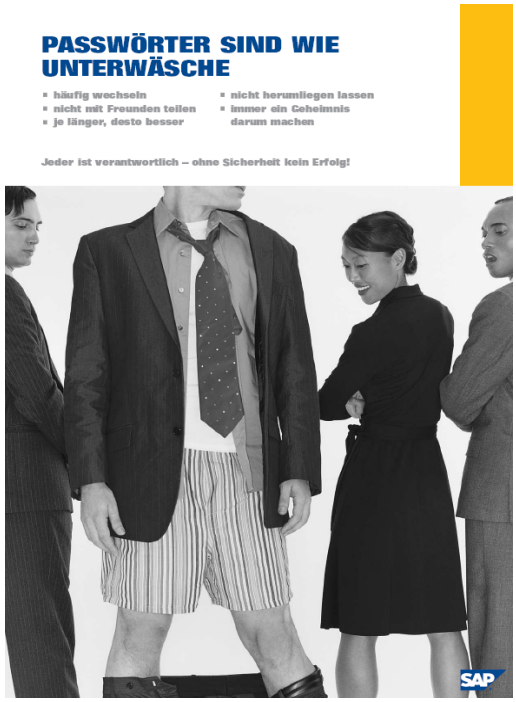
IWI Diskussionsbeiträge
 # 23 (5. Mai 2008)[1]
ISSN 1612-3646

Entwicklung von Security Awareness Konzepten unter Berücksichtigung ausgewählter Menschenbilder

Jörg Uffen[2], **Robert Pomes**[3], **Claudia M. König**[4] und **Michael H. Breitner**[5]





[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] Cand. Diplom-Ökonom, Wirtschaftswissenschaftliche Fakultät und Institut für Wirtschaftsinformatik, Leibniz Universität Hannover (j.uffen@web.de).
[3] Diplom-Ökonom und externer Doktorand, LG Electronics Deutschland GmbH, Willich (pomes@iwi.uni-hannover.de).
[4] Dr. paed., Coach, Video-Interaktions- und Management-Trainerin, Kommunikations- und Erziehungswissenschaftlerin, König Coaching Aachen und Hannover (www.coaching-koenig.com, koenig@coaching-koenig.com).
[5] Professor für Wirtschaftsinformatik und Betriebswirtschaftslehre und Direktor des Instituts für Wirtschaftsinformatik (breitner@iwi.uni-hannover.de).

Abstract

Die zunehmende Integration von Kunden, Lieferanten und Partnern in die Geschäftsprozesse von Unternehmen und allgemein von Organisationen aller Art macht die Sicherung und den Schutz der Informationssysteme immer wichtiger und auch komplexer. Unwissenheit oder leichte/grobe Fahrlässigkeit, aber auch Sabotage und Missbrauch, eigener Mitarbeiter stellen heute das größte Gefahrenpotential für Informationssysteme dar, während die Gefahr externer Angriffe durch Investitionen in Hard- und Software in den letzten Jahren abnahm. Das Risikomanagement fokussiert sich zunehmend auf das „Gefahrenpotential Mensch“: Die Sensibilisierung und vor allem die Motivation zum alltäglichen und allgegenwärtigen Mitdenken und Mitmachen steht im Mittelpunkt (Security Awareness Kampagne). Menschenbilder, z. B. des „Complex Man“, helfen für verschiedene Menschentypen verschiedene Anreizsysteme zu entwickeln, die sensibilisieren und motivieren. Diese Systeme mit positiven, aber auch negativen Anreizen (Sanktionen), sind die Basis für umfassende Security Awareness Konzepte, deren Entwicklung nachfolgend diskutiert und analysiert wird. Konkrete Handlungsempfehlungen für Unternehmen und Organisationen werden ausgearbeitet.

1 Einführung und Motivation

Die zunehmende Integration von Kunden, Lieferanten und Partnern in die Geschäftsprozesse von Unternehmen – und allgemein von Organisationen aller Art – macht die Sicherung der Informationssysteme immer komplexer und somit risikobehafteter. Im Blickpunkt steht heute vor allem der Bereich der IT-Compliance, d. h. die Einhaltung rechtlicher Vorgaben, die als entscheidende Kraft beim IT-Risikomanagement gilt [Pü07].

Die Bedrohung durch interne Angriffe hat schon seit einigen Jahren die Bedrohung durch Trojaner, Würmer oder Viren den Rang abgelöst. So konnte in mehreren Studien gezeigt werden, dass Unwissenheit oder Fahrlässigkeit in den eigenen Reihen der Unternehmen und Organisationen das größte Gefahrenpotential darstellt, während die Gefahr externer Angriffe durch verstärkte Investitionen in Hard- und Software innerhalb der letzten Jahre abnahm [Ke06]. Mitarbeiter sind i. d. R. zwangsläufig berechtigt, zumindest auf gewisse Bereiche eines internen Netzes zuzugreifen, wodurch sie mühelos an vertraulichen Daten und Informationen gelangen [Ha02]. Das IT-Risikomanagement fokussiert sich zunehmend auf die Reduktion des „Gefahrenpotentials Mensch“, so dass die konkrete Frage der Sensibilisierung der eigenen Mitarbeiter in den Vordergrund gerückt ist. Gezielt wird versucht mittels Spezialveranstaltungen, Seminaren oder Kampagnen die Bildung von Sicherheitsbewusstsein (neudeutsch: **Security Awareness**) bei den verschiedenen Mitarbeitern und Organisationsmitgliedern anzuregen.

Besonders zum „Thema Mensch“ gibt es eine Vielzahl von soziologischen und psychologischen Theorien und Modelle. Da der Mensch äußerst komplex ist, haben sich im Laufe der Jahre eine Vielzahl von Teildisziplinen entwickelt, die seine Verhaltensweisen soweit als möglich erklärbar und prognostizierbar machen. Eine dieser Disziplinen stellt die Organisationspsychologie dar, welche die Interaktion des Menschen in einer Organisation untersucht.
Um Security Awareness zu vermitteln, steht das Management der Informationssicherheit vor der Aufgabe, die verschiedenen Menschentypen in einer Organisation einzuschätzen, um anschließend darauf konkrete Motivationsstrukturen anzuwenden und deren Verhalten lenkbar und einschätzbar zu gestalten. In diesem Zusammenhang wird die Interdisziplinarität der Wirtschaftsinformatik bzw. genauer des Managements der Informationssicherheit zur Organisationspsychologie deutlich. Die Organisationspsychologie gibt einen konkreten Einblick in die Rolle, die Eigenschaften und Bedürfnisse, Motive, Erwartungen, sowie das Verhalten und die Einstellungen des Menschen in einer Organisation. Dies unterstreicht die Notwendigkeit der Heranziehung von in der Organisationstheorie angewandten Menschenbildern, um daraus normative Handlungsempfehlungen zur konkreten Steuerung von menschlichem Verhalten mit dem Ziel einer nachhaltigen Verbesserung der Informationssicherheit ermitteln zu können. Primäres Ziel dieses Aufsatzes ist es auf Basis verschiedener Menschenbilder ein konkretes, langfristiges und nachhaltiges Security Awareness Konzept vorzustellen.

2 Bedeutung der Informationssicherheit in Unternehmen

Auf Grund der starken Abhängigkeit der Organisationen von Informationssystemen, deren Ausfall zu unübersehbaren Ausfall- und sogar langfristigen Folgekosten führen kann, kommt dem Management der Informationssicherheit (u. a. CISO, CSO, evtl. auch CIO) eine immer zentralere Rolle zu. Es gilt vor allem die Grundeigenschaften der Informationssysteme bzgl. Informationssicherheit zu sichern.
Bei den Grundeigenschaften wird zwischen den semantischen Dimensionen der Verlässlichkeit und der Beherrschbarkeit unterschieden [Br05]. Erstere umfasst die Sicherheit der Informationen und Daten, wobei grundlegend die drei Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität [Br05;Ec06;Ker05] genannt werden. Beherrschbarkeit dagegen beschreibt die Sicherheit der betroffenen Kunden, Lieferanten und Mitarbeiter und unterscheidet als semantische Dimensionen die Revisionsfähigkeit sowie die Zurechenbarkeit [Br05].
Um reibungslose und ordnungsgemäße Prozesse zu gewährleisten, muss im Rahmen der IT-Governance ein Sicherheitskonzept – i. d. R. basierend auf einer Sicherheitsleitlinie und Sicherheitsgrundsätzen, die hier nicht näher betrachtet werden können – in einer Organisation vorhanden sein. Dieses Konzept muss neben den technischen auch die juristischen, wirtschaftlichen und organisatorischen bzw. personellen Aspekte [Kl04] umfassen. Stetige Audits, um ein gefordertes Mindestmaß an Informationssicherheit zu gewährleisten, sind unabdingbar. Die Ergebnisse des Audits stehen dem Management der Informationssicherheit zur Risikokontrolle und -reduktion zur Verfügung.

3 Menschen in Unternehmen und Organisationen

3.1 Theorie pluralistischer Menschenbilder

Ein Vertreter der Theorie der pluralistischen Menschenbilder war u. a. Edgar Schein[1]. Schein entwickelte nach der historischen Entwicklung vier Menschenbildtypen, die in dieser Reihenfolge wiedergegeben werden. Mit dem „**Rational-economic Man**" übernimmt Schein die Annahmen der von McGregor[2] entwickelten Theorie X. Die Theorie X, die zu der dualistischen Menschenbildtypologie gehört, sieht dem Menschen in einer Organisation pessimistisch entgegen. Arbeit wird als Leid angesehen und wird gezielt versucht zu umgehen [Sc03;St99]. Dieser bedarf somit einer strengen Führung und Kontrolle, um die Unternehmensziele zu erreichen [Sz94]. Darüber hinaus wollen Menschen keine Verantwortung übernehmen, sind wenig ehrgeizig und ziehen die Bewältigung von Routineaufgaben vor [MG70]. Der Mensch ist als passiv anzusehen, seine Empfindungen und Handlungen sind irrational, so dass es zu verhindern gilt, dass sie den rationalen Interessen eines Unternehmers entgegenstehen [St99;Sk05].
Ein derart pessimistisches Bild ließ sich nicht lange halten, so dass man im weiteren Zeitverlauf die Wichtigkeit in den sozialen Bedürfnissen des Menschen (sog. „**Social Man**") sah. Der Mensch versucht soziale Bedürfnisse zu befriedigen, da er Teil eines sozialen Systems ist [Be06]. Arbeit wird beim „Social Man" oft als sinnentleert betrachtet, so dass der Mensch primär nach sozialen Kontakten am Arbeitsplatz strebt, um eine Ersatzbefriedigung zu erhalten. Hierbei kommt vor allem die Kommunikation am Arbeitsplatz mit Kollegen sowie die Zusammenarbeit in Gruppen in Betracht, wobei der Mensch durch die soziale Kraft seiner Arbeitsgruppe gelenkt wird [St99;Sk05].
Im weiteren Zeitverlauf erfolgte die Erkenntnis, dass der Mensch nach Selbstverwirklichung strebt („**Self-actualizing Man**"). Die menschlichen Bedürfnisse sind in einer Hierarchie anzuordnen, die z. B. nach Maslow von den physiologischen Bedürfnissen über Sicherheitsbedürfnisse, soziale und Geltungsbedürfnisse bis hin zu Selbstverwirklichungsbedürfnissen reichen[3]. Der Mensch entwickelt sich durch den Arbeitsprozess stets weiter und will Verantwortung übernehmen. Es existiert kein Konflikt zwischen der Selbstverwirklichung und der Erreichung unternehmerischer Ziele [Sz94]. Schein´s Annahmen liegen nahe der McGregor´schen Theorie Y, die als Gegensatz der Theorie X betrachtet werden kann. Sofern sich ein Mensch mit den jeweiligen Zielen seines Unternehmens identifizieren kann, wird dieser zur Selbstkontrolle und Eigeninitiative tendieren. Überwachung und Strafe spielen nur eine untergeordnete Rolle [Sz94].
Schein sieht heute den Menschen als komplexes Wesen („**Complex Man**"), der äußerst wandlungs- und anpassungsfähig ist. Er lernt dauerhaft dazu und kommt auf Grund von Erfahrungen zu veränderten bzw. neuen Motiven. Des Weiteren ist die nach Maslow entwickelte Hierarchie der Bedürfnisse des Menschen nicht zu erkennen. Vielmehr stehen sie in einem kontinuierlichen Wandlungsprozess [St99;Sk05].

---

[1] Schein, Edgar (geb. 1928 in Zürich), Professor für Organisationspsychologie und Management am Massachusetts Institute of Technology (MIT) /Cambridge U.S.A.
[2] McGregor, Douglas (geb. 1906 in Detroit ✞1964 in Massachusetts), Professor für Management am MIT/Cambridge U.S.A.
[3] Siehe z. B. die Maslow´sche Bedürfnispyramide

Eine Verallgemeinerung des in einer Organisation vorherrschenden Menschenbildes lässt sich demzufolge nicht durchführen. Der Mensch kann situations-, typ- oder altersbedingt besonders passiv agieren oder auch nach sozialen Kontakten oder mehr Autonomie streben, d. h. auch wenn Schein den Menschen heute als komplexes Wesen ansieht, schließt er die übrigen Menschenbilder nicht kategorisch aus [St99]. Ein verallgemeinertes Führungsverhalten gibt es beim „Complex Man“ nicht, vielmehr gilt es Kombinationsmöglichkeiten aus Führungstheorien und unter Beachtung des Menschen Führungsverhalten zu generieren und individuell anzupassen, um aus Fähigkeiten, Motiven und Führungsnormen ein gezieltes Verhalten hervorzurufen [Sn80;Sz94].

3.2. Identifikation mit Informationssicherheit durch umfassende Anreizsysteme

Die Frage, warum ein Mitarbeiter oft grob oder leicht fahrlässig mit der Informationssicherheit umgeht, bezieht sich auf die Frage nach der Motivation eines Mitarbeiters. Das Verhalten eines Mitarbeiters muss vom Management derart gelenkt werden, dass das Verhalten den Zielen und Wünschen der Führung möglichst gerecht wird. Dies geschieht mittels der Gestaltung eines umfassenden Anreizsystems. Die am häufigsten in der Literatur zitierte Definition des Begriffs Anreizsystem stammt von Wild. Dieser definiert ein Anreizsystem als „die Summe aller bewusst gestalteten Arbeitsbedingungen, die bestimmte Verhaltensweisen (durch positive Anreize, Belohnungen etc.) verstärken, die Wahrscheinlichkeit des Auftretens anderer dagegen mindern (negative Anreize, Sanktionen)“ [Br90;Wi73].
Anreize müssen dazu führen, dass die Motive (Verhaltensbereitschaften) zu einem bestimmten zielgerichteten Verhalten gelenkt werden [Br90], was als Motivation bezeichnet wird [St99]. Staehle unterscheidet zwischen intrinsischer und extrinsischer Motivation [Be06;Br90;St99]. Man spricht von intrinsischer Motivation, wenn ein Mitarbeiter aus der Verrichtung einer Aufgabe eine Befriedigung erzielt, z. B. indem ein Programm erfolgreich installiert wurde [St99]. Werden die Anreize, welche einen Mitarbeiter zu einem bestimmten Verhalten lenken, durch ein umfassendes Anreizsystem erfasst, so spricht man von extrinsischer Motivation. Extrinsische Motive hängen von Verstärkern ab, die von außen hinzugeführt werden [St99]. Hierbei wird zwischen materiellen und immateriellen Motiven unterschieden [Br90]. Exemplarische immaterielle Motive sind der Wunsch nach Sicherheit, Kontakten oder Karriere, während materielle Motive z. B. monetäre Zusatzleistungen darstellen (siehe Abb. 1).
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. Die Frage, ob ein Unternehmen – oder allgemein eine Organisation – idealerweise ein extrinsisches Anreizsystem, eine intrinsische Ausgestaltung oder eine Kombination aus beiden einsetzt, ist mit den jeweiligen Unternehmenszielen und den Menschenbildern abzustimmen.
Schein´s Menschenbild des „Rational-economic Man“ ist durch monetäre Anreize motivierbar [Sn80]. 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 sein.

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
				soziale	Führungsstil, vorbildliche symbolische Führung, Partizipation, Kommunikation usw.
				organisatorische	Unternehmensimage, Arbeitszeitsystem, Unternehmenskultur, Karriereanreize usw.
		extrinsische	**mat.**	**direkte**	Entlohnung, Prämienzahlungen, Erfolgsbeteiligungen usw.
				indirekte	Firmenwagen, vergünstigte Essensausgabe usw.
	NEG.				betriebliche Haftungsregelungen betriebliche Disziplinarmaßnahmen

Abbildung 1: Betriebliche Anreize im Überblick. Quelle: in Anlehnung an Gunter et al. in [Th06], S. 16, sowie Seidel in [Sch91], S. 183.

Beim „Social Man“ lösen Gruppenanreizsysteme die individuell monetären ab. Die Bedürfnisbefriedigung von Anerkennung, Zugehörigkeitsgefühl und Identität stehen hierbei im Vordergrund, d. h. die zwischenmenschlichen Beziehungen in einem Unternehmen – und allgemein in einer Organisation – müssen gezielt verbessert werden, um Arbeitszufriedenheit zu gewährleisten [Sn80]. Bei dieser Art von Menschentyp muss der Focus 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 [Mö00]. Die Isolation eines Mitarbeiters kann dadurch verhindert werden. Weiterhin wichtig ist eine Einbindung der Mitarbeiter bei bestimmten Entscheidungen, was zu einer verstärkten Identifikation des Mitarbeiters mit dem Unternehmen führen kann und somit einen Beitrag zu mehr Zufriedenheit darstellt.
Der „Self-actualizing Man“ ist vor allem mittels intrinsischer Anreize zu motivieren, so dass die Arbeit selbst von innen heraus zur Motivation des Mitarbeiters führt. Die Delegation[4] von Entscheidungen spielt in diesem Sinne eine wichtige Rolle [Be06], um zu mehr Autonomie und Mitbestimmung zu gelangen. Der Manager wird somit nicht als Motivator oder Kontrolleur betrachtet, sondern als Unterstützer und Förderer [Sn80].
Die Gestaltung von Anreizen beim „Complex Man“ ist komplexer als bei den übrigen Menschenbildern. Auf Grund der erfahrungsbedingten ständigen Veränderungen und Anpassungen der Motive muss ein individuelles Maß an Anreizen gesetzt werden, die

[4] Unter Delegation versteht man die Übertragung von Kompetenzen (Rechte, Vollmachten) der Unternehmensspitze an hierarchisch untergliederte Stellen im Unternehmen [Be06]

sich situationsbedingt ändern. Manager agieren somit als Diagnostiker von Situationen, die Unterschiede erkennen und ihr eigenes Verhalten situationsbedingt variieren [Sn80;St99]. Die Zufriedenheit sowie eine damit zusammenhängende gute Leistung eines Mitarbeiters wird folglich nicht nur über die Motivation erreicht, denn Aspekte wie z. B. die Aufgabenverteilung, eigene Fähigkeiten und die Erfahrungen spielen ebenfalls eine wichtige Rolle [Sk06]. Die hohe Flexibilität eines Anreizsystems ist als besonders wichtig zu betrachten, um dauerhaft den verschiedenen Gegebenheiten stand zu halten [Br90].

Menschenbilder	**Eigenschaften**	**Anreizsysteme**
Economic Man	- Mensch ist passiv und manipulierbar - Mensch hat irrationale Gefühle	monetäre und v. a. negative Anreizsysteme
Social Man	- Motivation durch soziale Bedürfnisse - Arbeit ist sinnentleert, soziale Kontakte geben Ausgleich	Gruppenanreizsysteme, v. a. soziale Anreize
Self-actualizing Man	- es existiert eine Hierarchie der Bedürfnisse, wobei Selbstverwirklichung oft die zentrale Rolle zukommt - streben nach Autonomie, Selbstkontrolle sowie Selbstmotivation	Intrinsische Anreize
Complex Man	- Mensch ist komplex, wandlungs-, anpassungs- und lernfähig - sein Verhalten divergiert abhängig vom Reifegrad - keine klare Hierarchie der Bedürfnisse erkennbar	Individuell angepasste Anreizsysteme; es existiert keine einfache, allgemeine Führungsstrategie; situative Führung hilfreich

Tabelle 1: Menschenbilder und dessen Anreizsystem. Quelle: in Anlehnung an [Sz94], deutlich erweitert durch die Autoren.

4 Konkrete Handlungsempfehlungen zur mitarbeitersensitiven Erhaltung und Verbesserung der Informationssicherheit

Nachdem über die verschiedenen Menschenbilder und Unterschiede in der Motivierbarkeit diskutiert wurde, werden die Ergebnisse zu Handlungsempfehlungen für ein umfassendes Risikomanagement zusammengefasst.

Jede technische Sicherheitsmaßnahme wird nur so gut zur Anwendung kommen, wie ein Mitarbeiter tatsächlich mit ihr umgehen kann. Der Aspekt des Sicherheitsbewusstseins der Mitarbeiter – die Security Awareness – gewinnt somit zunehmend an Bedeutung [Fe05]. Diese Entwicklung ist klar durch diverse Informationssicherheitsstudien erkennbar. CA[5] zeigte mit einer 2006 durchgeführten Studie, dass die Bedrohung durch interne Angriffe am höchsten sei (64%). Die größten Risiken gehen hierbei von unsicheren Kennwörtern oder fehlender Nachvollziehbarkeit von Zugriffsberechtigungen der eigenen Mitarbeiter aus [CA07]. Diese Ergebnisse konnten durch eine kes-Studie[6] unterstrichen werden. Demzufolge gaben 52%[7] der Befragten an, dass das mangelnde Bewuss-

[5] CA = Computer Associates, eines der weltgrößten Unternehmen für IT-Management-Software
[6] kes: Fachzeitschrift für Informationssicherheit
[7] Mehrfachnennungen waren möglich

tsein der eigenen Mitarbeiter die Verbesserung der betrieblichen Informationssicherheit am meisten behindert. Nur die oftmals kritisierten knappen Budgets für Informationssicherheit konnten dies mit 54% Nennung noch übersteigen.
Ein probates Mittel zur **Mitarbeitersensibilisierung** und somit zur **Bewusstseinsbildung** ist die Durchführung einer Awareness-Kampagne [Fo04]. Eine derartige Kampagne muss über die Managementgrundfunktionen Planung, Organisation, Führung und Kontrolle [Se05] konstruiert werden. Die Kampagne muss dazu dienen Sicherheitsbewusstsein zu fördern und aufrecht zu erhalten. Das Ziel ist eine Kampagne in einer Organisation umzusetzen, in der z. B. mittels einer Schulung möglichst viel Wissen zur Informationssicherheit generiert werden muss.
Den Kern einer derartigen Kampagne stellt ein umfassendes, schriftlich fixiertes **Informationssicherheitskonzept** dar, in dem die Sicherheitsziele eines Unternehmens spezifiziert werden und die damit im Einklang stehenden Verhaltensanweisungen der Mitarbeiter dargestellt werden. Liegt kein Konzept vor, so besteht die erste Aufgabe in der Erstellung eines derartigen Konzeptes[8]. Die Anreizstrukturen eines Mitarbeiters sind unter Anwendung des jeweiligen vorherrschenden Menschenbildes in jeder Funktionsstufe des Managements einzubetten, um ein stetig hohes Motivationsniveau zu erreichen und damit das Handeln eines Mitarbeiters positiv zu beeinflussen (Abb. 2.0). Dargestellt werden der **Motivationsgrad** der Mitarbeiter in Abhängigkeit von der Ausgestaltung der vier Management Grundfunktionen.
Beim heute vorherrschenden Menschenbild des „Complex Man“ ist es wichtig, situativ ein hohes Maß an vielseitigen Anreizen in die Kampagne zu integrieren.

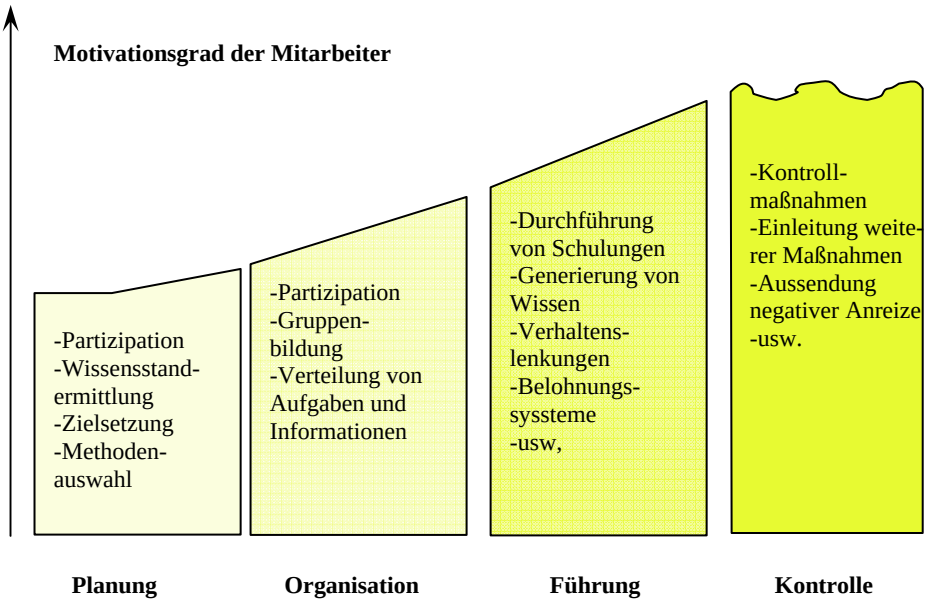


Abbildung 2: Managementkonzept zur Motivationssteigerung. Quelle: eigene Darstellung.

[8] Dies ist insbes. auch aus rechtlicher Sicht für das Unternehmen relevant, vgl. die verschärfte persönliche Haftung der Unternehmensleitung und siehe auch Einleitung

4.1. Managementaufgabe Planung

Die Motivation kann bereits in der Planungsphase einer Security Awareness Kampagne geweckt und gesteigert werden. Nach einer umfassenden **Ist-Analyse** (Risiken und Bedrohungen, insbes. auch Abschätzung der Schadensfolgen und -höhen) sowie einer **Bedarfsanalyse** werden die einzelnen Ziele dieser Kampagne definiert und mit dem Informationssicherheitskonzept abgestimmt. In der Bedarfsanalyse muss auch der Wissensstand der Mitarbeiter im Bezug zur Informationssicherheit ermittelt werden. Dies kann z. B. mittels eines kurzen Fragebogens an die Mitarbeiter erfolgen. Hier wird bereits ein erster Anknüpfungspunkt zur Motivationssteigerung erkennbar. Der „Complex Man" Mitarbeiter, der einen Fragebogen zum eigenen Wissensstand über Informationssicherheit ausfüllt, wird zum einen die Relevanz der Informationssicherheit feststellen, zum anderen durch die Fragestellungen bemerken, dass eigene Wissenslücken vorhanden sind. Dem pluralistischen Menschenbildtypus zufolge werden einige Mitarbeiter von sich aus versuchen, sicherheitsbewusster ihre Aufgaben zu bewältigen, indem z. B. Recherche über die Informationssicherheit betrieben wird oder sich mit anderen Organisationsmitgliedern ausgetauscht wird. Wie beschrieben wird sich dieses Verhalten nicht bei jedem Organisationsmitglied einstellen, so dass weitere Motivationsmöglichkeiten berücksichtigt werden müssen.
Demzufolge ist es wichtig, bereits bei der Planung einer Security Awareness Kampagne die Mitarbeiter im Entscheidungsprozess einzubinden und somit ihre Motivation durch Identifikation und Akzeptanz zu steigern. Diverse Rahmenbedingungen führen dazu, dass keine Akzeptanz der Informationssicherheit vorhanden ist und somit die Einsicht zu einer notwendigen Umsetzung von Informationssicherheitsmaßnahmen fehlt. Beim „Complex Man" ist die Motivierbarkeit verantwortungsbewusst mit der IT eines Unternehmens umzugehen am größten, sofern aus Mitarbeitersicht eine Mitverantwortung als auch eine angemessene Beteiligung am Unternehmenserfolg wahrgenommen wird [He05]. Die **Unternehmensidentifikation** spielt somit eine entscheidende Rolle dieses Menschenbildes, sich als Mitarbeiter für die Organisationsziele einzusetzen. Identifikation in diesem Kontext bezeichnet die Verbundenheit oder auch die Selbstverpflichtung eines Mitarbeiters mit einem Unternehmen [Bn06]. Ein hoher Identifikationsgrad eines Organisationsmitgliedes mit einem Unternehmen wird sich u. a. in hoher Einsatzbereitschaft und Motivation niederschlagen [Bn06]. Die Motivierung muss demzufolge auf dem Konzept der Identifikation aufbauen [He05]. Es ist möglich, sie bei der Zielsetzung zu integrieren oder sie bei der anschließenden Methoden- oder Medienauswahl einzubinden. Dies kann sich auch effizienzsteigernd auf die getroffenen Maßnahmen auswirken, da die Mitarbeiter vorhandenes Wissen oder neue Ideen in die Kampagne einbringen. Darüber hinaus steigt die Bereitschaft, die Vorgaben und Maßnahmen tatsächlich umzusetzen [BS07]. Zu den weiteren Aufgaben, die in der Planungsphase bewältigt werden müssen, zählen u. a. die Abstimmung mit anderen Unternehmensbereichen, wie z. B. mit der Controlling Abteilung.

4.2. Managementaufgabe Organisation

Eine signifikante Steigerung des Motivationspotentials muss in der Organisationsphase[9] erreicht werden, in der die Umsetzung der eigentlichen Kampagne erfolgt. Die Mitarbeiterpartizipation ist auch hier besonders wichtig, zum einen weil durch die Einbindung der Mitarbeiter weitere Wege zur Erreichung der Mitarbeiter erzielt werden und zum anderen, weil sich die Mitarbeiter eines Unternehmens so ständig mit dem Thema der Informationssicherheit beschäftigen. Sie frischen ihr Vorwissen auf und lernen die Wichtigkeit des Themas für das Unternehmen einzuschätzen. Welches Unternehmen wird eine derartige Kampagne durchführen, in der es die Mitarbeiter so stark einbezieht, wenn Security Awareness nicht von so großer Relevanz wäre? Entsprechend dem Menschenbild des „Complex man" werden die Organisationsmitglieder dies bemerken und auf ihr Verhalten darauf abstimmen.
Neben der intrinsischen Mitarbeitermotivation spielt auch die extrinsische Motivation eine entscheidende Rolle. Es müssen sowohl immaterielle soziale Anreize, als auch organisatorische Anreize eingesetzt werden. Die direkte Kommunikation zur Managementebene führt zu einem stärkeren **Unternehmensintegrationsgefühl**, was zu einer verstärkten Identifikation führt. Darüber hinaus werden durch Gruppeneinteilungen oder der Zuteilung von Aufgaben und Funktionen während der Kampagne das Dazugehörigkeitsgefühl der Mitarbeiter weiter gestärkt. Ihre Bedürfnisse nach sozialen Kontakten sowie Selbstverwirklichung müssen so weit wie möglich berücksichtigt werden. Eine Vielseitigkeit der eingesetzten Anreizarten beim Menschenbild des komplexen Wesens ist nötig.

4.3. Managementaufgabe Führung

Eine weitere Managementaufgabe ist die Führung[10]. In dieser Phase erfolgt z. B. die konkrete Durchführung von Schulungen und Unterweisungen. Ziele sind, dass Mitarbeiter durch die Schulung neues Wissen generieren, vorhandenes Wissen auffrischen und die Bedeutsamkeit der Informationssicherheit im Unternehmen verstehen lernen. Mitarbeiter müssen lernen die teils schwerwiegenden Konsequenzen bei Fehlverhalten richtig einzuschätzen. Dies muss mittels gut gewählter Medien übermittelt werden. Von besonderer Wichtigkeit ist, dass sowohl lernpsychologische als auch didaktische Ansätze, auf das vorherrschende Menschenbild zugeschnitten, Berücksichtigung findet.
Durch das Vorhandensein eines **direkten Ansprechpartners**, z. B. eines CISO, CSO oder evtl. auch CIO[11], im Unternehmen werden mögliche Ängste im Umgang mit der Informationssicherheit überwunden. Ein ansprechendes Belohnungssystem kann die Motivation eines Mitarbeiters in dieser Phase weiter steigern. Möglich wären der Einsatz direkter materieller Anreize, indem z. B. Prämien für besonders engagierte Mitarbeiter

[9] Organisation bedeutet in diesem Zusammenhang ein Mittel zur Umsetzung und Erreichung von Unternehmenszielen. [St99]
[10] Führung ist in diesem Kontext nicht gleichzusetzen mit der Leitung eines Unternehmens, sondern wird als Durchführung der Kampagne verstanden
[11] Idealerweise ist ein CIO nicht Hauptverantwortlicher für Informationssicherheit, da ein Zielkonflikt zwischen Effizienz und Effektivität (CIO) und ausreichenden Mindestsicherheitsstandards (CISO/CSO) besteht.

gezahlt werden, oder indirekte materielle Anreize. Zu diesen zählen z. B. die Verteilung von Mousepads für den privaten Haushalt mit Informationssicherheitsaufdrucken oder die Verteilung kostenloser Anti-Viren Software für den Privatgebrauch. In dieser Phase wird durch die Vielzahl der eingesetzten Motivationsstrukturen die höchste Motivationssteigerung eintreffen, u. a. auch auf Grund des bei der Schulung generierten Wissens. Selbstentfaltung und auch Selbstmotivation müssen entscheidende Berücksichtigung finden.

4.4. Managementaufgabe Kontrolle

Die vierte Managementaufgabe stellt die Kontrolle dar: Es muss gezielt kontrolliert werden, ob die Ziele erreicht werden und ob somit das Konzept erfolgreich umgesetzt wird, oder ob noch weiterer Handlungsbedarf existiert. Die Motivation der Mitarbeiter wird in dieser Phase nicht weiter steigen, sondern auf einem – möglichst hohen – Niveau bleiben. Dies lässt sich wie folgt erklären: Nach Schulungen usw. wird die Motivation der Mitarbeiter abnehmen, da einige Informationssicherheitsmaßnahmen in Vergessenheit geraten oder sich wieder kleine Nachlässigkeiten und leichte Fahrlässigkeiten einstellen. Um Nachhaltigkeit zu gewährleisten ist es wichtig Maßnahmen zu ergreifen, um den Erinnerungswert an die Kampagne und deren Ziele aufrecht zu erhalten. Möglich wären z. B. Poster mit Sprüchen zur Informationssicherheit, die im Unternehmen aufgehängt werden (siehe Abb. 3) oder ein Widererkennungszeichen in Form eines Logos oder Ähnliches, welches als Hintergrundbild auf dem PC gespeichert wird.

Abbildung 3: Erinnerungswertgestaltung mittels einer Poster-Kampagne.
Quelle: www.fiducia.de (Bild links); www.sap.de (Bild rechts).

Eine weitere „Motivationsmöglichkeit“ ist die Aussendung negativer Anreize in Form von Sanktionen, die motivationssteigernd wirken können. Falls es zu Sanktionen z. B. in Form einer Abmahnung kommt, zeigt dies auch auf weitere Mitarbeiter Wirkung, da diese Sanktionen umgehen wollen, so dass sicherheitsbewussteres Handeln gefördert wird. Die Kontrolle kann allerdings auch durch Selbstkontrolle erfolgen, indem durch ein E-Learning Modul das Wissen des Mitarbeiters über Informationssicherheit abgefragt wird und auf Basis der anschließenden Auswertung weitere Handlungsempfehlungen und Verbesserungsvorschläge unterbreitet werden.
Eine klare Trennlinie zwischen den Managementfunktionen kann nicht gezogen werden, d. h. einzelne Phasen, Aufgaben und Maßnahmen sind funktions- und zeitübergreifend. Ein umfassendes Anreizsystem muss, um ein nachhaltiges Sicherheitsbewusstsein im Unternehmen zu wecken, sowohl intrinsische Anreize als auch extrinsische Anreize enthalten. Jede Organisation gestaltet die entsprechenden Anreize so, dass sie genau auf vorhandene Menschenbilder abgestimmt werden, denn Unternehmen haben völlig verschiedene Mitarbeiter sowie verschiedene Informationssicherheitsbedürfnisse und -ziele. Weiterhin müssen im Unternehmen didaktische, pädagogische und kommunikative Kompetenzen vorhanden sein [Fo04], um einen Mitarbeiter entscheidend zu beeinflussen und sein Verhalten entscheidend zu ändern. Nur wenn dies alles Berücksichtigung findet und auch individuell im Unternehmen umgesetzt wird, kann die erwünschte Motivationswirkung dauerhaft erfolgreich erzielt werden.

5 Fazit und Ausblick

Menschen in Unternehmen und Organisationen sind komplexe Wesen, die durch verschiedene Persönlichkeiten, Fähigkeiten und Motive geprägt werden („Complex Man“). Es gibt keine allgemeine Führungsstrategie für Menschen in Unternehmen – und allgemein in Organisationen aller Art. Deshalb ist es vor allem im äußerst sensiblen Bereich der Informationssicherheit notwendig eine möglichst hohe Bandbreite an Anreizen zu setzen, um möglichst alle von der Relevanz der Informationssicherheit zu überzeugen und zum Mitmachen zu motivieren. Für das Risikomanagement bedeutet dies u. a. zunächst die Gefahr, die von den eigenen Mitarbeitern ausgeht, einzuschätzen und anschließend Handlungsbedarf aufzuzeigen. Eine Security Awareness Kampagne ist oft eine sehr gute Maßnahme. Jede Managementgrundfunktion ist dabei wichtig, wobei stets eine starke Einbindung der Mitarbeiter erfolgen muss, um eine starke Identifikation mit der Kampagne und dem Unternehmen zu erzeugen. Das Risikomanagement steht vor der umfassenden Aufgabe, für die verschiedenen Menschenbildtypen Anreize zu konstruieren, um auch nach der Kampagne ein notwendiges Mindestsicherheitsbewusstsein zu erhalten. Es zeigt sich, dass zunehmend mehr Unternehmen derartige Kampagnen durchführen. Ein bekanntes Beispiel hierfür ist T-Systems mit der Kampagne „Mission Security“, die nach eigenen Angaben einen großen Erfolg erzielen konnte.

6 Literaturverzeichnis

[Be06] Bea, F.; Göbel, E.: Organisation. Lucius & Lucius, Stuttgart 2006, (3. Aufl.), S. 302, S. 339 f.

[Br90] Becker, F.: Anreizsysteme für Führungskräfte. Poeschel, Stuttgart 1990 (1. Aufl.), S. 8 – 47.

[Br05] Breitner, M.; Pomes, R.: IT-Sicherheit – Kein Selbstzweck, sondern Notwendigkeit. In: IZN Mail Ausgabe 4, Oktober 2005, S. 24.
[Bn06] Bröckermann, R.: Handbuch Personalentwicklung: die Praxis der Personalentwicklung, Personalförderung und Arbeitsstrukturierung. Schäffer–Poeschel, Stuttgart 2006 (1. Aufl.), S. 247 f., S. 400ff.
[BS07] BSI (Bundesamt für Sicherheit in der Informationstechnik): BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise. URL: http://www.bsi.de/literat/bsi_standard/standard_1002.pdf, 2007, Download: 24.5.2007.
[CA06] CA (Computer Associates): Studie IT-Sicherheit 2006/2007 – Herausforderung Compliance. URL: http://www.caemea.com/de/papers/studie_it-sicherheit_2006_ 2007.pdf , S. 13. Download: 21.8.2007.
[Ec06] Eckert, C.: IT-Sicherheit: Konzepte, Verfahren und Protokolle. Oldenbourg, München 2006, (4. Aufl.), S. 49.
[Fe05] Ferstl, O.; Sinz, E.; Eckert, S.; Isselhorst, T.: Wirtschaftsinformatik 2005. Physica-Verlag Heidelberg, Heidelberg 2005 (1. Aufl.), S. 1228.
[Fo03] Fox, D.: Security Awareness – Oder die Wiederentdeckung des Menschen in der IT-Sicherheit. URL: http://www.secorvo.de/publikationen/security-awareness-fox-2003.pdf, 2003, S. 678. Download: 23.5.2007.
[Ha02] Hansen, H. R.; Neumann, G.: Wirtschaftsinformatik Arbeitsbuch. Lucius & Lucius, Stuttgart 2002 (6. Aufl.), S. 1266.
[He05] Hentze, J., et al.: Personalführungslehre – Grundlagen, Funktionen und Modelle der Führung. Haupt, Bern 2005 (4. Aufl.), S. 161 – 163.
[Ker05] Kersten, H.; Klett, G.: Der IT Security Manager: Expertenwissen für jeden IT-Manager. Vieweg-Verlag, Wiesbaden 2005 (1. Aufl.), S. 41.
[Ke06] kes/Microsoft: Sicherheitsstudie 2006 – Lagebericht zur Informationssicherheit. S. 6, www.kes.de.
[Kl04] Klostermann, C.: IT-Sicherheit in kleinen und mittelständischen Unternehmen. DIHK Verlag, Berlin 2004 (1. Aufl.), S.13.
[MG70] McGregor, D.: Der Mensch im Unternehmen. Econ, Düsseldorf 1970 (1. Aufl.), S.47f.
[Mö00] Möller, I.: Produktivitätswirkungen von Mitarbeiterbeteiligungen. URL: http://doku.iab.de/mittab/2000/2000_4_MittAB_Moeller.pdf, 2000 (33. Jg.), S.567. Download: 24.5.2007.
[Pü07] Pütter, C.: Compliance treibt Risikomanagement voran. URL: http://www.cio.de/financeit/analysen/834189/index.html. Download: 22.8.2007.
[Sch91] Schanz, G.: Handbuch Anreizsysteme. Poeschel, Stuttgart 1991 (1. Aufl.).
[Sn80] Schein, E.: Organisationspsychologie. Gabler, Wiesbaden 1980 (1. Aufl.), S. 50 ff..
[Sz94] Scholz, C.: Personalmanagement: informationsorientierte und verhaltenstheoretische Grundlagen. Vahlen, München 1994 (4. Aufl.), S. 405 – 407.
[Sc03] Schreyögg, G.: Organisation: Grundlagen moderner Organisationsgestaltung. Berlin 2003 (4. Aufl.), S. 226.
[St99] Staehle, W.: Management. Vahlen, München 1999 (8. Aufl.), S. 166, S. 192 – 195, S. 216ff., S. 249, S.671.
[Se05] Steinle, C.: Unterlagen zur Vorlesung „Planung & Organisation“. Hannover, SS 2005, S. 2.
[Sk05] Stock, M.: Unterlagen zur Vorlesung „Einführung in die wirtschaftswissenschaftliche Genderforschung“. URL: http://www.uni-graz.at/margareta.kreimer/going-gender/ Bildung-und-Gender.pdf, 2005, S. 6. Download: 5.5.2007.
[Th06] Thom, N.; Zaugg, R.: Moderne Personalentwicklung – Mitarbeiterpotentiale erkennen, entwickeln und fördern. Gabler, Wiesbaden 2006 (1. Aufl.).
[Wi73] Wild, Jürgen: Organisation und Hierarchie. In: Zeitschrift Führung und Organisation, (42. Jg), 1973, Nr. 1 S. 45 - 54

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.

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.