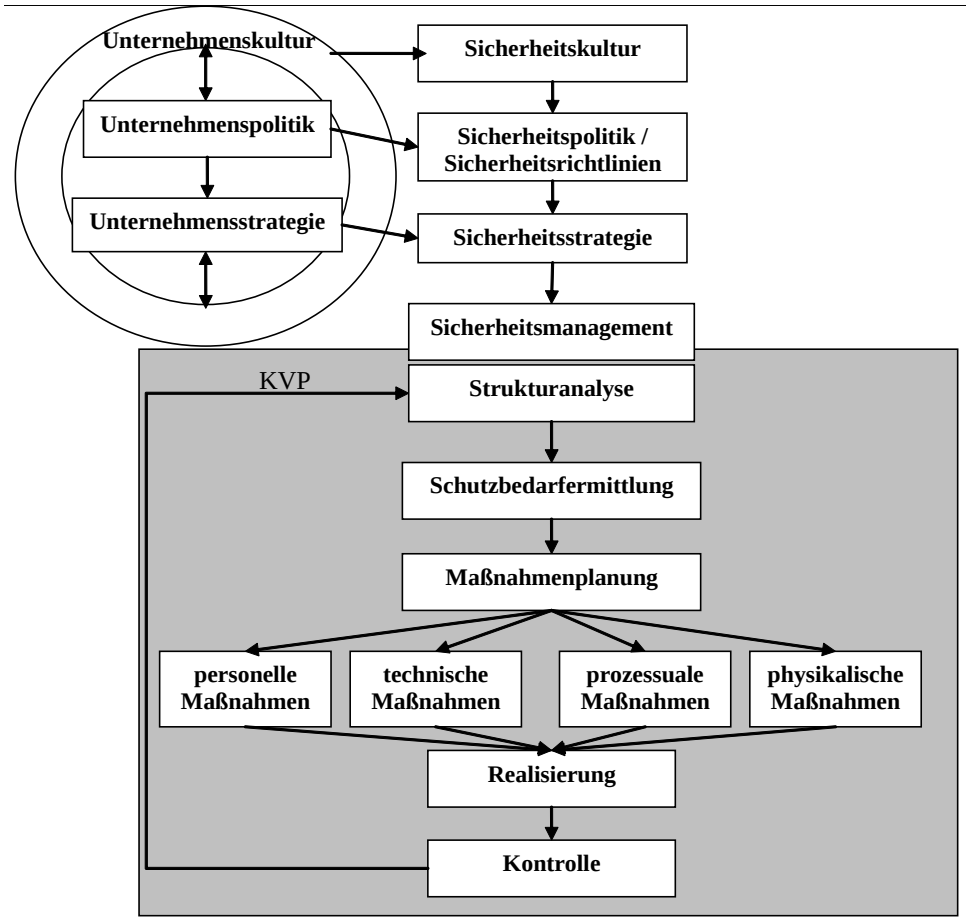
IWI Diskussionsbeiträge
39 (03. Februar 2010)[1]

ISSN 1612-3646

Ein ganzheitliches Konzept für Informationssicherheit unter besonderer Berücksichtigung des Schwachpunktes Mensch

Björn Semmelhaack[2], **Jon Sprenger**[3] und **Michael H. Breitner**[4]



[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] Diplom-Ökonom, NORD/LB, Friedrichswall 10, 30159 Hannover (bjoern.semmelhaack@nordlb.de).

[3] Diplom-Ökonom, wissenschaftlicher Mitarbeiter und Doktorand (sprenger@iwi.uni-hannover.de).

[4] Professor für Wirtschaftsinformatik und Betriebswirtschaftslehre und Direktor des Instituts für Wirtschaftsinformatik der Leibniz Universität Hannover (breitner@iwi.uni-hannover.de).

1 Notwendigkeit der Informationssicherheit in einem Unternehmen

Informationen und Daten sind ein sensibler Faktor eines Unternehmens. Schutzmaßnahmen der Informationstechnik (IT) werden jedoch in vielen Unternehmen vernachlässigt.[5] Es bedarf einer adäquaten Informationssicherheit, die garantiert, dass Informationen verfügbar sind, jedoch lediglich für autorisierte Stellen.

Informationssicherheit besteht aus der IT-Sicherheit (Informations- sowie Datenschutz) und aus dem Schutz der IT-Technik. Zur Informations- und Datenverarbeitung werden Hardware- und Softwarekomponenten, Netzwerke sowie Menschen eingesetzt, die Schutz bedürfen. Der Mensch muss in ein geeignetes Sicherheitskonzept eingebunden werden, da der Mitarbeiter ein Risiko darstellt.[6] Mitarbeiter lassen sich idealtypisch in Menschenbilder eingruppieren,[7] so dass entsprechend differenziert auf diese eingegangen werden kann.

Informationssicherheit gilt es in der Unternehmenskultur zu verankern und in eine Sicherheitskultur einzubetten. Essentiell für die Informationstechnologie ist es, eine IT-Sicherheitsstrategie zu entwickeln.[8]

2 Basisanforderungen an die Informationssicherheit

Tabelle 1: Definitionen und rechtliche Grundlagen

Sicherheit	*Sicherheit* bezeichnet „den Zustand des Sicherseins vor Gefahr oder Schaden bzw. einen Zustand, in dem Schutz vor Gefährdungen besteht. […] Die Sicherheit zu einem bestimmten Zeitpunkt wird als **Ist-Sicherheit** bezeichnet und ist von einem geplanten Ausmaß an Sicherheit, der **Soll-Sicherheit**, zu unterscheiden.“[9]
***Informationssicherheit* (engl. security)**	*Informationssicherheit* (engl. security) beschreibt „die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen.“[10]
Datensicherheit	*Datensicherheit* definiert „die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen. Damit umfasst die so beschriebene Sicherheit der Daten insbesondere auch Maßnahmen zur Datensicherung (engl. backup), also den Schutz vor Datenverlust durch Erstellung von Sicherheitskopien.“[11]
IT-Sicherheit	„Sicherheit in der Informationstechnik […] bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen • in informationstechnischen Systemen oder Komponenten oder • bei der Anwendung von informationstechnischen Systemen oder Komponenten“.[12] Nach dieser Definition bezweckt die IT-Sicherheit, durch rechtliche, technische und organisatorische Maßnahmen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Informationen bzw. Daten sicherzustellen.[13]
Compliance	„Übereinstimmung mit geltenden Vorgaben.“[14] Die Compliance wird von der Unternehmensführung vorangetrieben. Ziel ist die Einhaltung gesetzlicher Vorschriften und interner Vorgaben oder Beschlüssen von Aufsichtsbehörden.

[5] Vgl. Lassmann (2006), S. 349.
[6] Vgl. Schlienger (2007), S. 487; Mix/Pingel (2007), S. 498; Zerr (2007), S. 519; Fox (2003), S. 676; Schimmer (2007), S.510; Baier/Straub (2005), S. 313; Fox/Kaun (2005), S. 329; Schultz (2005), S. 426.
[7] Vgl. Schein (1980), S. 52.
[8] Vgl. von Solms/von Solms (2004), S. 372.
[9] Hoppe/Prieß (2003), S. 23 (Hervorhebungen im Original).
[10] Eckert (2008), S. 5.
[11] Ebenda.
[12] BSI-Einrichtungsgesetz vom 17. Dezember 1990 (BGBI I S. 2834), zuletzt geändert 2003 (BGBI. I S 2304).
[13] Vgl. Reinhard (2007), S. 37.
[14] Pohlmann (2008), S. 1.

oder durch bessere ersetzt werden. Diese gesammelten Daten werden im ISM aufbereitet und ausgewertet, um die Schutzmaßnahmen und die gesamte Informationssicherheit zu steigern. Auch die Sicherheitsziele, die Sicherheitsstrategie und das Sicherheitskonzept sind auf deren Korrektheit und Umsetzbarkeit zu prüfen und an die neuen Veränderungen anzupassen.[267]
Für die Abweichungskontrolle bietet sich ein Sicherheitscheck mittels eines IT-Security Audits an, um Abweichungen von berichteten und vom tatsächlichen IST-Zustand, auf der Basis einer zuvor festgelegten Checkliste, zu ermitteln. Die ermittelten Abweichungen (Findings) sind in einem Audit-Report zu dokumentieren. Der auditierte Bereich sollte zu den Abweichungen aus seiner Sicht Stellung nehmen können und die Gründe hierfür darlegen.[268]
Die Kontrolle dient weiterhin der Überprüfung der Angemessenheit und Wirksamkeit der Schutzmaßnahmen.[269] Wird eine Abweichung festgestellt, so sind die abweichenden Maßnahmen zu verbessern oder durch andere zu ersetzen, um das angestrebte Sicherheitsniveau zu erreichen.

7 Fazit und Ausblick

Die Brisanz des Themas Informationssicherheit und der Einfluss der Menschen auf diese sowie die Abhängigkeit von der IT sind für Unternehmen von großer Bedeutung, denn eine Vernachlässigung der Informationssicherheit kann zu gravierenden Konsequenzen führen.
Die internen Bedrohungen durch den menschlichen Risikofaktor lassen sich verringern, indem die einzelnen Mitarbeiter entsprechend ihres Menschenbildes durch Anreize motiviert werden, sich sicherheitskonform zu verhalten. Ferner gilt, es eine Sinnvermittlung der Sicherheit durch Etablierung einer unternehmensweiten Sicherheitskultur zu schaffen und die Mitarbeiter durch Awareness Kampagnen für die Informationssicherheit zu sensibilisieren. Das adäquate Verhalten und die nötige Qualifikation im Umgang mit der Informationssicherheit können durch Schulungen erlernt und trainiert werden, jedoch können auch bereits vor der Einstellung durch geeignete Verfahren wie AC und Arbeitsproben die Einstellung zur Informationssicherheit geprüft und in Folge dessen sicherheitsbewusste Mitarbeiter rekrutiert werden.
Die Manager sind Teil der Mitarbeiterschaft und müssen ebenso gezielt an die Informationssicherheit durch oben genannte Maßnahmen herangeführt werden, um die Wichtigkeit und die daraus resultierenden Folgen einschätzen zu können. Die Brisanz der Informationssicherheit und aller damit verbunden Konsequenzen müssen von den Managern erkannt werden, damit entsprechende Budgets für Schutzmaßnahmen bereitgestellt werden. Ihre Vorbildfunktion den Mitarbeitern gegenüber können sie nur dann erfüllen, wenn sie selber den sicherheitskonformen Umgang mit den Systemen, Daten und Informationen vorleben, an Schulungen teilnehmen, bei der Erstellung einer Sicherheitskultur aktiv beteiligt sind und die Mitarbeiter situativ führen sowie sie bei ihrer tagtäglichen Arbeit unterstützen.
Es obliegt den Managern, die Budgets für die Schutzmaßnahmen freizugeben, dabei sollte jedoch auf deren Wirtschaftlichkeit geachtet werden. Schon 20% der Schutzmaßnahmen können einen 80%-igen Schutz bieten, wobei jedes weitere Prozent exponentiell ansteigende Kosten verursacht[270] und folglich eine 100%-ige Sicherheit nicht zu realisieren ist.[271]

[267] Vgl. BSI (2008a), S. 82.
[268] Vgl. Schmidt (2007), S. 527.
[269] Vgl. Hofmann (2007a), S. 260.
[270] Vgl. Pohlmann (2006), S. 28f.

Ein effizienter Schutz ist nur durch eine Realisierung von personellen, technischen, prozessualen und physikalischen Maßnahmen in Verbindung mit einem Sicherheitsmanagement, der dazugehörigen Sicherheitspolitik und schriftlich fixierten Sicherheitsrichtlinien zu gewährleisten, um sowohl interne als auch externe Bedrohungen zu minimieren. Eine einseitige Investition in beispielsweise nur technische oder prozessuale Maßnahmen würde das schwächste Glied, den Menschen, nicht berücksichtigen und somit ineffizient sein. Die Wechselwirkungen zwischen den Maßnahmen sind zu berücksichtigen. Nur wenn diese Bedingungen erfüllt sind, kann das Business Continuity durch das richtige Verhalten der Mitarbeiter gewährleisten werden, um finanzielle Schäden aber auch Reputationsschäden zu vermeiden.
Das vorliegende Sicherheitskonzept geht verstärkt auf die personellen Maßnahmen ein, da sie in den Unternehmen stark vernachlässigt werden, obwohl sie die Sicherheit deutlich erhöhen können. Im Rahmen dieser Arbeit ist es jedoch nicht möglich, alle Facetten der möglichen Schutzmaßnahmen zu erörtern. Zudem ist das Konzept noch in der Praxis zu überprüfen.
ITIL als good practice De-facto-Standard vermittelt ein gutes Rüstzeug für die Informationssicherheit, jedoch werden die personellen Maßnahmen nur unzureichend berücksichtigt. Aus diesem Grund wurde das Information-Security Management in ITIL V3 durch das vorgestellte ganzheitliche Sicherheitskonzept bezüglich der personellen und technischen wie aber auch der physikalischen Maßnahmen erweitert und ergänzt. Damit ist ein größerer Schutz vor dem Risikofaktor Mensch gegeben.

Die Bedrohungen der Informationssicherheit werden auch in Zukunft existent sein, wobei sich jedoch die Art ändern kann. Neue Techniken und Verfahren werden auch zukünftig für Bedrohungen sorgen, denen wiederum durch neue technische, prozessuale, physikalische aber auch personelle Maßnahmen zu begegnen ist. Für die Informationssicherheit besteht kontinuierlich Forschungsbedarf, um gegen die Bedrohungen effiziente und kostengünstige oder kostengünstigere Maßnahmen zu entwickeln.
Um die Sicherheitseinstellung der Mitarbeiter zu ermitteln, müssen Verfahren für Interviews, Assessment-Center und Praktika entwickelt werden, die die Validität der Einstellung ermitteln können. Damit könnten Unternehmen in der Lage sein, Mitarbeiter einzustellen, die sich sicherheitskonform verhalten werden und zum Schutz der Informationssicherheit, ihrer Systeme, Daten und Informationen beitragen. Eine Weiterbildungen im Rahmen der Informationssicherheit sollte in regelmäßig erfolgen. Wie solche Schulungen oder Fortbildungen am effizientesten zu gestalten sind, ist noch zu entwickeln.
Die Informationssicherheit darf letztlich nicht in ein Zwangssystem ausarten, welches die Individualität und die Identität der Mitarbeiter ausschließt. Hierzu bedarf es weiterer Forschung, die der Entmenschlichung des Arbeitsplatzes entgegengewirkt, indem z. B. im Rahmen der Unternehmens- und Sicherheitskultur private Dinge auf dem PC zugelassen werden. Dies trägt dazu bei, einem Befreiungsschlag seitens der Mitarbeiter, bei dem sie die Informationssicherheit nicht beachten und Schäden anrichten, entgegen zu wirken.[272]

[271] Vgl. Humpert (2004), S. 16.
[272] Vgl. Pokoyski (2006), S. 1f.

Literaturverzeichnis

Ahrendts, F., Marton, A. (2008) IT-Risikomanagement leben! Wirkungsvolle Umsetzung für Projekte in der Softwareentwicklung, Springer Verlag, Berlin/Heidelberg 2008

Baier, H., Buchmann, J., Busch, C. (2003) Aus und Weiterbildung in IT-Sicherheit; in: IT-Sicherheit im verteilten Chaos - Tagungsband 8. Deutscher IT-Sicherheitskongress des BSI, SecuMedia Verlag, Ingelheim 2003, S. 179-190

Baier, H., Straub, T. (2005) Awareness by doing – ein neues Konzept zur Sensibilisierung von IT-Anwendern; in: IT-Sicherheit geht alle an! – Tagungsband zum 9. Deutschen IT-Sicherheitskongress, SecuMedia Verlag, Ingelheim 2005, S. 313-326

Becker, Fred G. (1990) Anreizsysteme für Führungskräfte: Möglichkeiten zur strategisch-orientierten Steuerung des Managements, Poeschel Verlag, Stuttgart 1990

Blickle, Gerhard (2004) Menschenbilder, in: Schreyögg/Werder (Hrsg.), Handwörterbuch Unternehmensführung und Organistaion, 4., völlig neu überarbeitete Auflage, Schäffer-Pöschel Verlag, Stuttgart 2004, Sp. 836-843

Bock, W., Macek, G., Oberndorfer, T., Pumsenberger, R. (2008) Praxisbuch ITIL: Erfolgreiche Zertifizierung nach ISO 20000, 2. aktuelle und erweiterte Auflage, Galileo Press, Bonn 2008

Böttcher, Roland (2008) IT-Servicemanagement mit ITIL® V3: Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen, 1. Auflage, Heise Verlag, Hannover 2008

Bon, Jan von (2008) IT-Service Management basierend auf ITIL V3 - Das Taschenbuch, itSMF Inernational, 1. Auflage, Van Haren Publishing, Zaltbommel 2008

Bruch, Heike (1996) Intra- und interorganisationale Delegation als Managementaufgabe: Entwicklung eines markt-, potential- und wertorientierten Modells, Dissertation; Universität Hannover, 1996

Brunnstein, Jochen (2006) ITIL Security Management realisieren: IT-Service Security Management nach ITIL – So gehen Sie vor, 1. Auflage, Vieweg & Sohn Verlag, Wiesbaden 2006

Buchsein, R., Victor, F., Günther, H., Machmeier, V. (2008) IT-Management mit ITIL® V3: Strategien, Kennzahlen, Umsetzung; 2., aktualisierte und erweiterte Auflage, Vieweg + Teubner Verlag, Wiesbaden 2008

Buhl, Ulrike (2008) ITIL Praxisbuch: Beispiele und Tipps für die erfolgreiche Prozessoptimierung, 2. Auflage, mitp Redline GmbH, Heidelberg 2008

Buerschaper, Cornelius (2008) Organisationen - Kommunikationssystem und Sicherheit, in: Badke-Schaub, P./Hofinger, G./Lauche, K. (Hrsg.), Human Factors: Psychologie sicheren Handelns in Risikobranchen, Springer Verlag, Berlin/Heidelberg 2008, S. 155-175

BSI (2005) IT-Sicherheit geht alle an! – Tagungsband zum 9. Deutschen IT-Sicherheitskongress, SecuMedia Verlag, Ingelheim 2005

Deci, E. L., Ryan, R. M. (1993) Die Selbstbestimmungstheorie und der Motivation und ihre Bedeutung für die Pädagogik, in: Zeitschrift für Pädagogik, 39. Jg. 1993 Nr. 2, S. 223-238

Drumm, Hans-Jürgen (2008) Personalwirtschaft, 6., überarbeitete Auflage, Springer Verlag, Berlin/Heidelberg 2008

Ebel, Nadin (2008) ITIL® Basis-Zertifizierung: Grundlagen und Zertifizierungsvorbereitung für die ITIL® Foundation-Prüfung, Addison-Wesley-Verlag, München 2008

Eckert, Claudia (2008) IT-Sicherheit: Konzepte – Verfahren – Protokolle, 5., überarbeitete Auflage, Oldenbourg Verlag, München 2008

Engelkamp, P., Sell, F. L. (2005) Einführung in die Volkswirtschaftslehre, 3., verbesserte Auflage, Springer Verlag, Berlin Heidelberg 2005

Eschweiler, J., Psille, D. (2006) Security@Work: Pragmatische Konzeption und Implementierung von IT-Sicherheit mit Lösungsbeispielen auf Open Source Basis, Springer Verlag, Berlin/Heidelberg 2006

Falke, Ulrich (2003) Scheinbar sicher- Eine Zusammenfassung von Ergebnissen aktueller Befragungen und Expertengespräche, in: Gora, W./Krampert, T. (Hrsg.), Handbuch IT-Sicherheit: Strategien, Grundlagen und Projekte, Addison-Wesley-Verlag, München 2003, S. 181-196

Fox, Dirk (2003) Security Awareness oder: Die Wiederentdeckung des Menschen in der IT-Sicherheit; in: Datenschutz und Datensicherheit 27 (2003) 11, 2003, S. 676-680

Fox, D., Kaun, S. (2005) Security Awareness Kampagnen, in: IT-Sicherheit geht alle an! – Tagungsband zum 9. Deutschen IT-Sicherheitskongress, SecuMedia Verlag, Ingelheim 2005, S. 329-337

Friberg, C., Gerhardt, C, Luttenberger, N. (2003) Die Integration von Schutzbedarfsanalysen und IT-Grundschutz nach BSI, in: Gora, W./ Krampert, T. (Hrsg.), Handbuch IT-Sicherheit: Strategien, Grundlagen und Projekte, Addison-Wesley-Verlag, München 2003, S. 65-79

Gabriel, Roland (2006) IT-Sicherheit und Data Warehousing; in: Chamoni, P./Gluchowski, P. (Hrsg.), Analytische Informationssysteme: Business Intelligence-Technologie und -Anwendungen, dritte, vollständig überarbeitete Auflage, Springer Verlag, Berlin/Heidelberg 2006, S. 439-450

Geiger, Gebhard (2007) IT-Sicherheit als integraler Bestandteil des Risikomanagements im Unternehmen, in: Gründer, T./Schrey, J. (Hrsg.), Managementhandbuch IT-Sicherheit: Risiken, Basel II, Recht, Erich Schmidt Verlag, Berlin 2007, S. 27-51

Gründer, Torsten (2007) IT-Controlling mit Service Level Agreements SLA Performance Cycle (SLAPeC), in: Gründer, T./Schrey, J. (Hrsg.), Managementhandbuch IT-Sicherheit: Risiken, Basel II, Recht, Erich Schmidt Verlag, Berlin 2007, S. 235-247

Hansen, H. R., Neumann G. (2005a) Wirtschaftsinformatik 1: Grundlagen und Anwendungen, 9. Auflage, Lucius & Lucius Verlagsgesellschaft mbH, Stuttgart 2005

Hansen, H. R., Neumann G. (2005b) Wirtschaftsinformatik 2: Informationstechnik, 9. Auflage, Lucius & Lucius Verlagsgesellschaft mbH, Stuttgart 2005

Heinrich, L. J., Heinzl, A., Roithmeyer, F. (2007) Wirtschaftsinformatik: Einführung und Grundlegung, dritte, vollständig überarbeitete und ergänzte Auflage, Oldenbourg Verlag, München 2007

Hentze, J., Graf. A., Kammel, A., Lindert, K. (2005) Personalführungslehre: Grundlagen, Funktionen und Modelle der Führung, 4., neu bearbeitete Auflage, Haupt Verlag, Berlin/Stuttgart/Wien 2005

Hersey, P., Blanchard, K. (1982) Management of Organizational Behaviour: Utilizing Human Resources, fourth edition, Prentice Hall, London et al., 1982

Hesch, Gerhard (1997) Das Menschenbild neuer Organisationsformen: Mitarbeiter und Manager im Unternehmen der Zukunft, Gabler Verlag, Wiesbaden 1997

Hofmann, Jürgen (2007) IT-Organisation und Personal, in: Hofmann, J./Schmidt, W. (Hrsg.), Masterkurs IT-Management: Das Wissen für die erfolgreiche Praxis - Grundlagen und beispielhafte Umsetzung - Für Studenten und Praktiker, 1. Auflage, Vieweg & Sohn Verlag, Wiesbaden 2007, S. 91-140

Hofmann, Jürgen (2007a) IT-Sicherheitsmanagement, in: Hofmann, J./Schmidt, W. (Hrsg.), Masterkurs IT-Management: Das Wissen für die erfolgreiche Praxis - Grundlagen und beispielhafte Umsetzung - Für Studenten und Praktiker, 1. Auflage, Vieweg & Sohn Verlag, Wiesbaden 2007, S. 233-274

Holey, T., Welter, G., Wiedemann, A. (2004) Wirtschaftsinformatik, Friedrich Kiehl Verlag, Ludwigshafen (Rhein) 2004

Hoppe, G., Prieß, A. (2003) Sicherheit von Informationssystemen: Gefahren, Maßnahmen und Management im IT-Bereich, nwb Verlag, Herne/Berlin 2003

Humpert, Frederik (2004) IT-Sicherheit, in: HMD Praxis der Wirtschaftsinformatik 236, 2004, S. 7-18

Hungenberg, H., Wulf, T. (2007) Grundlagen der Unternehmensführung, 3., aktualisierte und erweiterte Auflage, Springer Verlag, Berlin Heidelberg, New York 2007

Jung, Hans (2006) Personalwirtschaft, 7., überarbeitete Auflage, Oldenbourg Verlag, München 2006

Kirchler, E., Meier-Pesti, K., Hofmann, E. (2004) Menschenbilder in Organisationen, WUV - Universitätsverlag, Wien 2004

Köhler, R.-D., Krampert,T., van Hülsen, E. (2003) Von der IT-Sicherheitsanforderung zum Service Level Agreement, in: Gora, W./Krampert, T. (Hrsg.), Handbuch IT-Sicherheit: Strategien, Grundlagen und Projekte, Addison-Wesley-Verlag, München 2003, S. 333-352

Kopperger, D., Kunsmann, J., Weisbecker, A. (2007) IT-Servicemanagement, in: Tiemeyer, E. (Hrsg.), Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, Carl Hanser Verlag, München/ Wien 2007, S. 121-257

Krcmar, Helmut (2005) Informationsmanagement, 4., überarbeitete und erweiterte Auflage, Springer Verlag, Berlin/Heidelberg, 2005

Lardschneider, Martin (2008) Social Engineering: Eine ungewöhnliche aber höchst effiziente Security Awareness Maßnahme; in: Datenschutz und Datensicherheit (DuD), 09/2008, S. 574-578

Lassmann, Wolfgang (2006) Kapitel 9 IT-Sicherheit in; Lassmann, W. (Hrsg.): Wirtschaftsinformatik Nachschlagewerk für Studium und Praxis; 1. Auflage, Gabler Verlag, Wiesbaden 2006 S. 349-408

Lehner, F., Wildner, S., Scholz, M. (2007)Wirtschaftsinformatik: Eine Einführung, Carl Hanser Verlag, München/Wien, 2007

Matthiesen, Kai H. (1995) Kritik des Menschenbildes in der Betriebswirtschaftslehre: Auf dem Weg zu einer sozialökonomischen Betriebswirtschaftslehre, Haupt Verlag, Bern/Stuttgart/Wien 1995

Mertens, P., Bodendorf, F., König, W., Picot, A., Schumann, M. (2001) Grundzüge der Wirtschaftsinformatik, 7., neu bearbeitete Auflage, Springer Verlag, Berlin/Heidelberg/New York, 2001

Mix, M., Pingel, M. (2007) Be Better – Be Sure: Security Awareness in der Bosch Gruppe; in: Datenschutz und Datensicherheit (DuD) 31 (2007) 7, 2007, S. 498-501

Müller, Klaus-Rainer (2005) IT-Sicherheit mit System: Sicherheitspyramide und Vorgehensmodelle - Sicherheitsprozess und Katastrophenvorsorge – Die 10 Schritte zum Sicherheitsmanagement, 2., verbesserte und aktualisierte Auflage, Vieweg und Sohn Verlag, Wiesbaden 2005

Münch, Isabel (2007) IT-Grundschutz zum Bewältigen von IT-Risiken in Unternehmen; in: Gründer, T./Schrey, J. (Hrsg.), Managementhandbuch IT-Sicherheit: Risiken, Basel II, Recht, Erich Schmidt Verlag, Berlin 2007, S. 285-308

Neuberger, Oswald (2002) Führen und führen lassen: Ansätze, Ergebnisse und Kritik der Führungsforschung, 6., völlig neu bearbeitete und erweiterte Auflage, Lucius & Lucius Verlag, Stuttgart 2002

Oechsler, Walter (2005) Personal und Arbeit: Grundlagen des Human Resource Management und der Arbeitgeber-Arbeitnehmer-Beziehung, 8., grundlegend überarbeitete Auflage, Oldenbourg Verlag, München Wien 2005

OGC (2007a) Office of Government Commerce (OCG) (Hrsg.): ITIL Service Strategy, TSO (The Stationery Office), Crown Copyright, London 2007

OGC (2007b) Office of Government Commerce (OCG) (Hrsg.): ITIL Service Design, TSO (The Stationery Office), Crown Copyright, London 2007

Olbrich, Alfred (2008) ITIL kompakt und verständlich erklärt: Effizientes IT-Management – Den Standard für IT-Prozesse kennenlernen, verstehen und erfolgreich in der Praxis umsetzen, 4., erweiterte und verbesserte Auflage, Vieweg + Teubner Verlag, Wiesbaden 2008

Poguntke, Werner (2007) Basiswissen IT-Sicherheit: Das Wichtigste für den Schutz von Systemen & Daten, W3L-Verlag, Herdecke/Witten 2007

Pohl, Lorenz (2007) 2. Kapitel: Datenschutzrecht, Teil I: Rechtliche Aspekte der IT-Sicherheit; in: Reinhard/Pohl/Capellaro (Hrsg.), IT-Sicherheit und Recht: Rechtliche und technisch-organisatorische Aspekte für Unternehmen, Schmidt Verlag, Berlin 2007, S. 55-93

Pohlmann, Norbert (2003) Firewall-Systeme, 5. aktualisierte Auflage, mitp-Verlag, Bonn 2003

Pohlmann, Norbert (2006) Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen?, in: HMD Praxis der Wirtschaftsinformatik 248, 2006, S. 26-34

Pohlmann, Norbert (2008) Herausforderung Compliance, in: Pohlmann, Norbert (Hrsg.), Organisationshandbuch Netzwerksicherheit: Praxislösungen für den Netzwerkverantwortlichen Band 1, Weka Medien GmbH& Co. KG, Kissingen 2008, Teil2/6.2, S. 1-8

Pohlmann, N., Blumberg, H. (2006) Der IT-Sicherheitsleitfaden: Das Pflichtheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen, 2., aktualisierte Auflage, mitp-Verlag, Heidelberg 2006

Prottung, Stefan (2008) Auf dem Weg zur Geschäftsentwicklung mit der IT – Die innovative Kraft der IT für die Geschäftsentwicklung nutzen, in: Keuper F. /Schomann, M./ Grimm, R. (Hrsg.), Strategisches IT-Management: Management von IT und IT-gestütztes Management, 1. Auflage, Gabler / GWV Fachverlage GmbH, Wiesbaden 2008, S. 63-78

Raepple, Martin (2001) Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, 2. überarbeitete und erweiterte Auflage, dpunkt Verlag, Heidelberg 2001

Rauschen, T., Disterer, G. (2004) Identifikation und Analyse von Risiken im IT-Bereich, in: HMD Praxis der Wirtschaftsinformatik 236, 2004, S. 19-32

Reichenbach, Martin (2004) Sicherheitsmanagement und Versicherungsmöglichkeit, in: Ernst, Stefan (Hrsg.); Hacker, Cracker & Computerviren: Recht und Praxis der Informationssicherheit, OVS Verlag Dr. Otto Schmidt, Köln 2004, S. 329-353

Reinhard, Tim (2007) 1. Kapitel: Grundlagen; Teil I: Rechtliche Aspekte der IT-Sicherheit; in: Reinhard/Pohl/Capellaro (Hrsg.), IT-Sicherheit und Recht: Rechtliche und technisch-organisatorische Aspekte für Unternehmen, Schmidt Verlag, Berlin 2007, S. 37-47

Ridder, Hans-Gerd (2007) Personalwirtschaftslehre, 2., überarbeitete Auflage, Verlag W. Kohlhammer, Stuttgart 2007

Rosenstiel, Lutz von (1975) Die motivationalen Grundlagen des Verhaltens in Organisationen – Leistung und Zufriedenheit, Duncker & Humblot Verlag; Berlin 1975

Rotenstrauch, C., Schulze, T. (2003) Informatik für Wirtschaftswissenschaftler und Wirtschaftsinformatiker, Springer Verlag, Heidelberg/Berlin 2003

Schadt, Dirk (2006) Über die Ökonomie der IT-Sicherheit: Betrachtungen zum Thema »Return on Security Investment«, in: HMD Praxis der Wirtschaftsinformatik 248, 2006, S. 16-25

Schein, Edgar H. (1980) Organizational Psychology, 3rd edition, Prentice-Hall International, London 1980; deutsche Version: Organisationspsychologie, Gabler Verlag, Wiesbaden 1980

Schimmer, Klaus (2007) Sicherheit beginnt im Kopf: Sensibilisieren - aber wie?, in: Datenschutz und Datensicherheit 31 (2007) 7, 2007, S. 510-514

Schlienger, Thomas (2003) Sicherheitskultur: der Mensch in der Informationssicherheit, in: Switchjournal 1/2003, S. 34-37

Schlienger, T., Baur, C., Barau, S. et al. (2004) Leitfaden zur Förderung und Analyse der Informationssicherheitskultur: Abschlussbereicht der Arbeitsgruppe „Informationssicherheitskultur“ der FGSec fachlichen Sektion der Schweizer Informatik Gesellschaft, iimt University Press, Fribourg 2004

Schlienger, Thomas (2007) Informationskultur: Messung, Planung, Steuerung; in: Datenschutz und Datensicherheit (DuD) 31 (2007) 7, 2007, S. 487-491

Scholz, Christian (1994) Personalmanagement: Informationsorientierte und verhaltenstheoretische Grundlagen, 4., verbesserte Auflage, Franz Vahlen Verlag, München 1994

Scholz, Christian (2000) Personalmanagement: Informationsorientierte und verhaltenstheoretische Grundlagen, 5., neubearbeitete und erweiterte Auflage, Franz Vahlen Verlag, München 2000

Schreiber, Sebastian (2006) Kosten und Nutzen von Penetrationstest**,** in: HMD Praxis der Wirtschaftsinformatik 248, 2006, S. 86-91

Schultz, Eugene (2005) The human factor in security; in: Computers & Security (2005) 24, p. 425-426

Schwyter, F., Wisler, A. (2007) Informationssicherheit für KMU: Sicherheitskonzepte & praktische Umsetzung, BPX-Edition, Rheinfelden (Schweiz) 2007

Seibold, Holger (2006) IT-Risikomanagement, Oldenbourg Verlag, München Wien 2006

Solms, von / von Solms (2004) The 10 deadly sins of information security management; in: Computer & Security (2004) 23, p. 371-376

Sommer, Jochen (2004) IT-Servicemanagement mit ITIL® und MOF, 1. Auflage, mitp Verlag, Bonn 2004

Spector, Paul E. (1996) Industrial and organizational psychology: research and practice, John Wiley & Sons, New York [u. a.] 1996

Staehle, Wolfgang H. (1999) Management: Eine verhaltenswissenschaftliche Perspektive, 8. Auflage überarbeitet von Conrad, P. und Sydow, J., Verlag Franz Vahlen, München 1999

Stahlknecht, P., Hasenkamp, U. (2005) Einführung in die Wirtschaftsinformatik, elfte, vollständig überarbeitete Auflage, Springer Verlag, Berlin/Heidelberg 2005

Steinle, Claus (1978) Führung: Grundlagen, Prozesse und Modelle der Führung in der Unternehmung, C. E. Poeschel Verlag, Stuttgart 1978

Steinle, C., Ahlers, F. (2004) Menschenbilder, in: Gaugler, E./Oechsler, W./Weber, W. (Hrsg.), Handwörterbuch des Personalwesens, 3., überarbeitete und ergänzte Auflage, Schäffer-Poeschel Verlag, Stuttgart 2004, Sp. 1142-1151

Steinle, Claus (2007) Unternehmensführung – ein »grundlegender« Überblick; in: Steinle, C./Daum, A. (Hrsg.), Controlling: Kompendium für Ausbildung und Praxis, 4., überarbeitete Auflage, Schäffer-Poeschel Verlag, Stuttgart 2007

Suter, W. (1999) Motivation; in: Steiger, Th./Lippmann, E. (Hrsg.): Handbuch angewandte Psychologie für Führungskräfte: Führungskompetenz und Führungswissen, Springer Verlag, Berlin /Heidelberg 1999, S. 132-142

Swoboda, J., Spitz, S., Pramateftakis, M. (2008) Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen, 1. Auflage, Vieweg + Teubner Verlag, Wiesbaden 2008

Temme, Matthias (2004) (Un)-Sicherheitspotenzial Mitarbeiter, in: <kes> Die Zeitschrift für Informationssicherheit, Nr. 2, März 2004, S. 10-14

Töpfer, Armin (2005) Betriebswirtschaftslehre: Anwendungs- und prozessorientierte Grundlagen, Springer Verlag, Berlin/Heidelberg 2005

Tsintsifa, Lydia (2005) IT-Sicherheitskultur mit IT-Grundschutz, in: IT-Sicherheit geht alle an! – Tagungsband zum 9. Deutschen IT-Sicherheitskongress, SecuMedia Verlag, Ingelheim 2005, S. 219-228

Ulrich, Hans (1990) Unternehmenspolitik, 3. Auflage, Haupt Verlag, Bern, Stuttgart 1990

Uth, S., Demon, S., Petrov, W. (2008) Sicherheit an öffentlichen Computerarbeitsplätzen des CMS, in: cms-journal 30, Juni 2008, S. 38-41

Weinert, Ansfried B. (1995) Menschenbilder und Führung, in: Kieser (Hrsg.), Handwörterbuch der Führung, 2., neu gestaltete Auflage, Schäffer-Pöschel Verlag, Stuttgart 1995, Sp. 1495-1510

Weinert, Ansfried B. (2004) Organisations- und Personalpsychologie, 5., vollständig, überarbeitete Auflage, Beltz Verlag, Basel 2004

Wiltner, Frank (2003) Bedrohungen für Unternehmen, in: Gora, W./Krampert, T. (Hrsg.), Handbuch IT-Sicherheit: Strategien, Grundlagen und Projekte, Addison-Wesley-Verlag, München 2003, S. 81-96

Wunderer, Rolf (2007) Führung und Zusammenarbeit: Eine unternehmerische Führungslehre, 7., überarbeitete Auflage, Luchterhand Verlag, München 2007

Zarnekow, R./Brenner, W./Pilgrim, U. (2005) Integriertes Informationsmanagement: Strategien und Lösungen für das Management von IT-Dienstleistungen, Springer Verlag, Berlin/Heidelberg 2005

Zerr, Konrad (2007) Security-Awareness-Monitoring: Ein sozialwissenschaftlicher Ansatz zur Messung des Sicherheitsbewußtseins bei Mitarbeitern: in: Datenschutz und Datensicherheit 31 (2007) 7, 2007, S. 519-523

Onlinequellen:

Abawajy, J. H., Thatcher, K., Kim, T. (2008) Investigation of Stakeholders Commitment to Information Security Awareness Programs, in: International Conference on Information Security Assurance, p. 472-476, online unter: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4511613&isnumber=4511515 [13.01.2009]

Bitkom (o. J.) Sicherheit für Systeme und Netze in Unternehmen: Einführung in die IT-Sicherheit und Leitfaden für erste Maßnahmen, 2. überarbeitete Auflage, online unter: http://www.bitkom.org/de/themen_gremien/54746_38229.aspx [24.12.2008]

BSI (2007) Leitfaden IT-Sicherheit: IT-Grundschutz kompakt, unter : http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf [02.12.08]

BSI (2008a) BSI Standard 100-2: IT-Grundschutz-Vorgehensweise Version 2, unter http://www.bsi.bund.de/literat/bsi_standard/standard_1002.pdf [23.12.2008]

Deloitte (2007) 2007 Global Security Survey – The shifting security paradigm, 2007 unter http://www.deloitte.org/dtt/cda/doc/content/us_fsi-DeloitteGlobalSecuritySurvey2007.pdf [26.01.2009]

Dolya, Alexey (2007a) Interne IT-Bedrohung in Europa 2006, Infowatch, online unter: http://www.infowatch.com/de/threats?ipcountry=DE&chapter=162971949&id=26#it [20.11.08]

ohne Verfasser (2008) Lagebericht zur Informations-Sicherheit 1, in: <kes> Die Zeitschrift für Informationssicherheit, Nr.4, August 2008, online unter: http://www.kes.info/archiv/heft/abonnent/08-4/08-4-018.htm [28.01.2009]

Oltmann, Uwe (2008) Der VPN-Dienst an der Universität Hannover, online unter: http://www.rrzn.uni-hannover.de/index.php?id=141&no_cache=1&type=98 [21.01.09]

Pokoyski, Dietmar (2006) Entsicherung am Arbeitsplatz – Studie entschlüsselt erstmalig psychologische Wirkweisen und Zusammenhänge der IT-Security, online unter: http://www.securitymanager.de/magazin/artikel_1184-print_entsicherung_am_arbeitsplatz_studie.html [16.12.08]

Topf, Jochen (2005) Antispam-Strategien: Unerwünschte E-Mails erkennen und abwehren, Bundesamt für Sicherheit in der Informationstechnik, Bundesanzeiger, Köln 2005, online unter: http://www.bsi.bund.de/literat/studien/antispam/antispam.pdf [19.11.08]

Wieshoff, Rainer (2005) USB-Sperre: Übertriebenes Misstrauen oder legitime Vorsicht? unter: http://www.channelpartner.de/knowledgecenter/security/grundlagen/200997/ [03.12.08]

Wiedemann, Jochen (2007)

Gestaltung von IT-Notfallvorsorge im Kontext des Risikomanagements Teil2: Entwicklung von Gestaltungselementen am Beipiel einer TK-Unternehmung, Institut für Sicherheit im E-Business (ISEB), Nr. 27, unter http://www.iseb.ruhr-uni-bochum.de/download/ISEB-AB-27-Wiedemann_2.pdf, [17.11.08]

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 p., #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.

Jörg Uffen und Michael H. Breitner, *Stärkung des IT-Sicherheitsbewusstseins unter Berücksichtigung psychologischer und pädagogischer Merkmale*, 37 S., #36, 24. Oktober, 2009.

Christian Fischer und Michael H. Breitner, *MaschinenMenschen – reine Science Fiction oder bald Realität?,* 36 S., #37, 13. Dezember, 2009.

Tim Rickenberg, Hans-Jörg von Mettenheim und Michael H. Breitner, *Plattformunabhängiges Softwareengineering eines Transportmodells zur ganzheitlichen Disposition von Strecken- und Flächenverkehren,* 38 S., #38, 11. Januar, 2010.