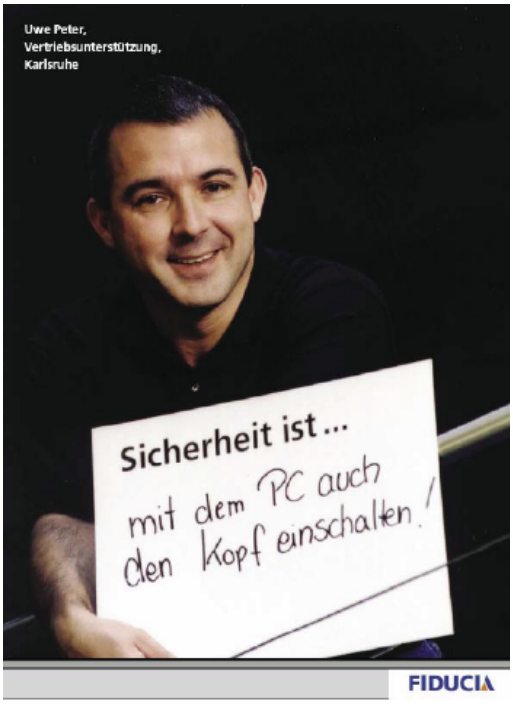
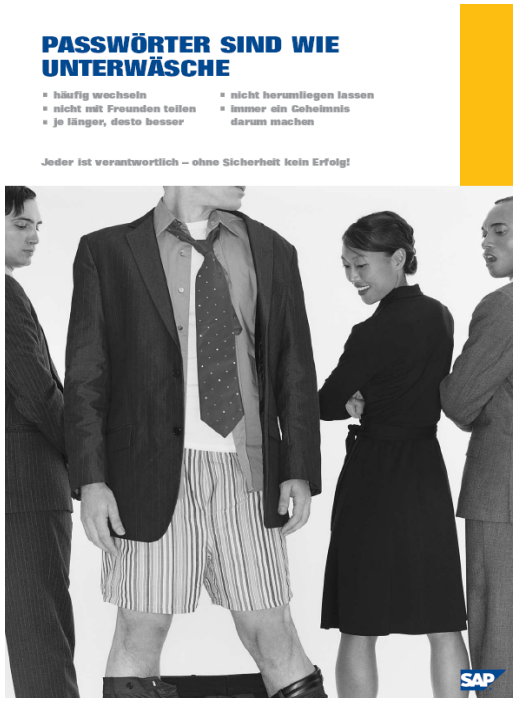
IWI Diskussionsbeiträge
 # 23 (5. Mai 2008)[1]
ISSN 1612-3646

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.

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.

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.