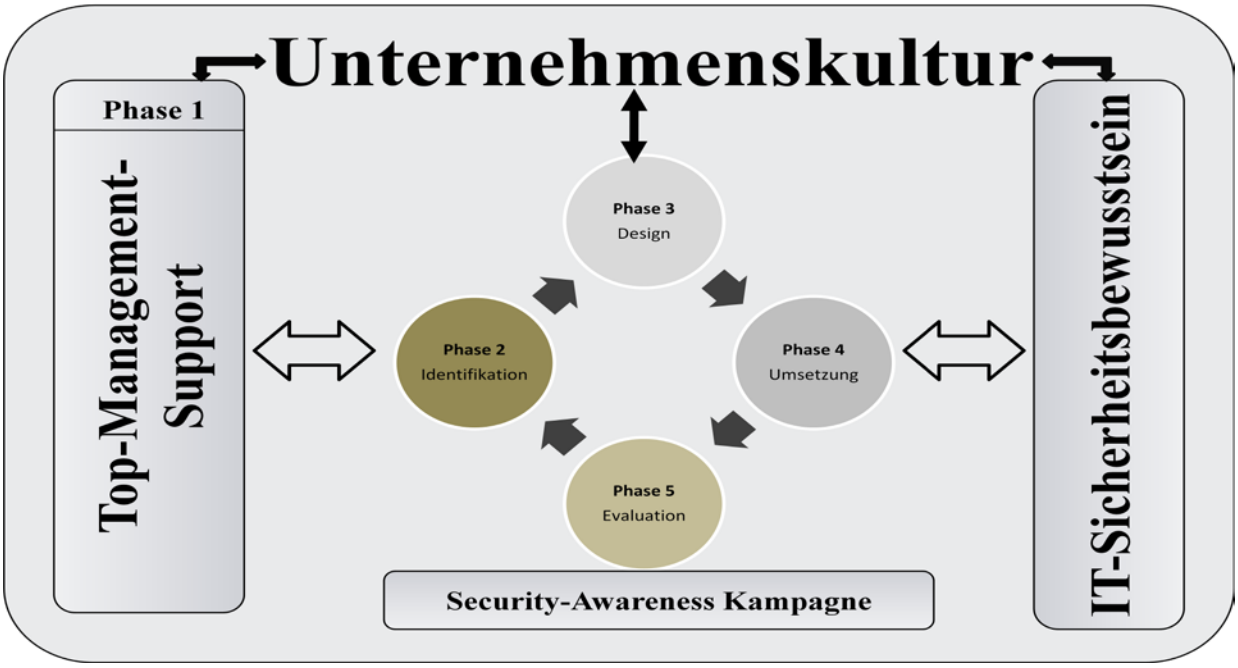
IWI Diskussionsbeiträge
 # 36 (24. Oktober 2009)[1]
ISSN 1612-3646

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.