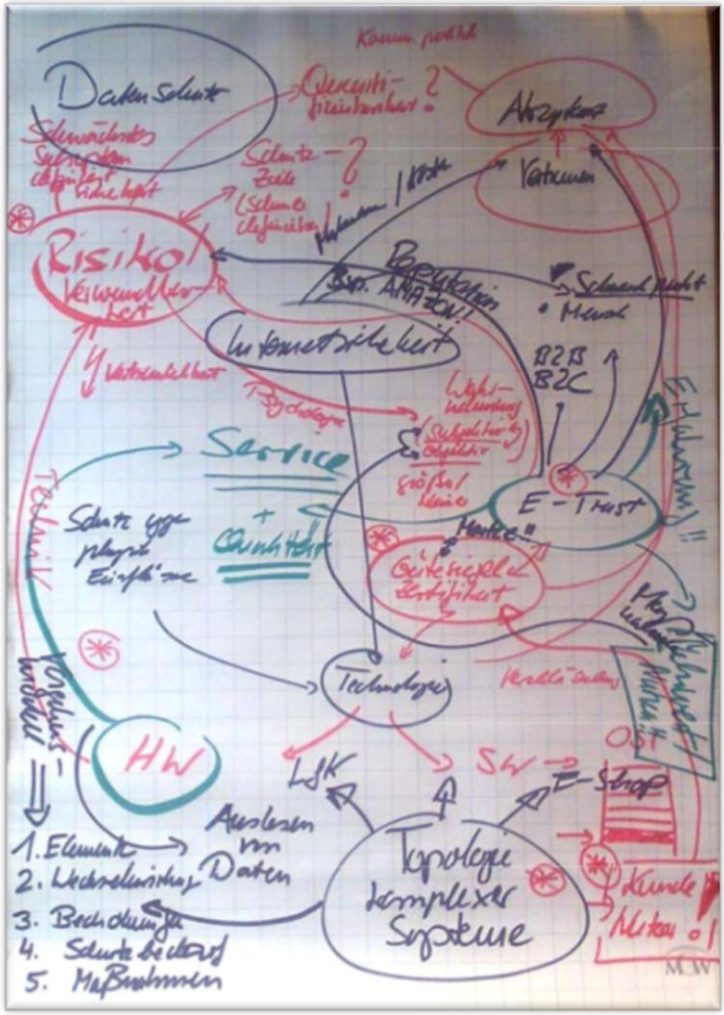
IWI Diskussionsbeiträge

32 (17. Februar 2009)[1]

ISSN 1612-3646

Entwicklung des Hannoveraner Referenzmodells für Sicherheit und Evaluation an Fallbeispielen

Sebastian Schmidt[2], **Hans-Jörg von Mettenheim**[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

[3] Diplom-Mathematiker, Diplom-Ökonom, Institut für Wirtschaftsinformatik (mettenheim@iwi.uni-hannover.de).

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

Inhaltsverzeichnis

Zusammenfassung

Spätestens seit den verheerenden Terroranschlägen vom 11. September 2001 gewinnt das Thema Sicherheit in Gesellschaft, Politik und Wissenschaft immer mehr an Bedeutung. Die Leibniz Universität Hannover hat aus diesem Grund die interdisziplinäre Forschungsinitiative zum Sicherheit unter der Leitung von Herrn Prof. Dr. Bach ins Leben gerufen. Ziel der Forschungsinitiative ist es, vorhandene technologische, naturwissenschaftliche sowie sozial- und geisteswissenschaftliche Kompetenzen zum Thema Sicherheit an der Leibniz Universität Hannover zu bündeln, um damit ein Forum für Fragen der Sicherheitsforschung zu schaffen, das sich besonders durch sein interdisziplinäres Profil auszeichnet.
Im Rahmen dieser Initiative haben sich Herr Prof. Dr. Breitner und Mitarbeiter des Instituts für Wirtschaftsinformatik mit der Entwicklung eines Referenzmodells Sicherheit befasst, um die komplexen Sachverhalte bei der Entstehung eines Sicherheitskonzeptes besser zu strukturieren und in zeitlich abgegrenzte Phasen zu unterteilen. Die Ergebnisse des ersten Brainstormings anlässlich eines Workshops am 10. Juli 2008 finden sich auf dem Deckblatt wieder. Bei einem zweiten Termin wurden die Gedanken weiter konkretisiert und das Modell grob entworfen. Dies ist in Abbildung 2 zu sehen.
Hauptanliegen der Arbeit ist, aus den ersten Ideen das sogenannte Hannoveraner Referenzmodell Sicherheit zu entwickeln, welches für möglichst viele Szenarien anwendbar sein soll. Zu diesem Zweck werden zuerst die relevanten Begriffe zum Thema Sicherheit definiert. Anschließend wird das grundlegende Modell in einer Abbildung dargestellt, um dann Schritt für Schritt ausführlich erläutert zu werden. Den Überlegungen des Modells folgend wird ein Excel-Tool erstellt, das über die Auswahl von Bedrohungen und Schwachstellen zu möglichen Schutzmaßnahmen führt. Im Weiteren werden zwei Fallbeispiele aus den Bereichen Videoüberwachung und Wasserversorgung vorgestellt und das erstellte Excel-Tool an diesen Beispielen getestet. Es folgt eine Auswahl von Standards, Zertifikate und Gütesiegel. Abschließend wird ein Fazit gezogen und ein Ausblick in die Zukunft gegeben.

Wie die ISO 27001 basiert die ISO 9001 auf dem zyklischen PCDA-Modell.

Durch die Prozessorientierung der ISO 9001 eignet sie sich als Grundlage zur Integration verschiedener Managementsysteme, z.B. der ISO/IEC 27001. Die Prozesslandschaft würde wiederum im Mittelpunkt stehen und könnte um weitere Prozesse erweitert werden.[98]

5.4 Gütesiegel

Für Online-Shops existieren eine Reihe von Gütesiegeln, die eine Schlüsselinformation oder Qualitätssignale für den Verbraucher darstellen. Sie bündeln wichtige Informationen über die Leistungen und Qualität und sollen so den Verbraucher von der Informationssuche befreien.

Eine Definition für das Internet-Gütesiegel liefert Rüdiger:

„Internet-Gütesiegel sind im Rahmen einer Selbstregulierung von einer unabhängigen Institution herausgegebene Wort- und/oder Bildzeichen, die Online-Händler zur Kennzeichnung auf ihren Webseiten einsetzen und die gegenüber den Kunden bzw. potentiellen Kunden in verdichteter Form darüber Auskunft geben, dass der betreffende Online-Händler die vom Zeichengeber (in Form von Verhaltenskodizes, Kriterienkatalogen, Normen, Leitfäden o. Ä.) festgelegten Kriterien/(Qualitäts-)Anforderungen bezüglich seiner Geschäftspraktiken insbesondere im Hinblick auf die Informations-Privatheit, die IT-Sicherheit und den Verbraucherschutz einhält."[99]

Die Kriterien basieren neben europäischen und deutschen Gesetzen auch auf Empfehlungen von Verbraucherschützern. Sie verfolgen das Ziel, den Kunden des Online-Shops vor den typischen Risiken des Internetkaufs, z.B. Verstöße gegen Datenschutzbestimmungen, intransparente Preisangaben oder Einschränkungen des Widerrufsrechts zu schützen.[100]

6. Fazit und Ausblick

Sicherheit erlangt einen immer höher werdenden Stellenwert. Angesichts der Komplexität der Erstellung von Sicherheitskonzepten ist es sinnvoll, ein Referenzmodell zu entwickeln, das auf möglichst viele Situationen und Szenarien anwendbar ist.
Zu diesem Zweck wurde ausgehend von den Überlegungen von Prof. Dr. Breitner und seinen Mitarbeitern ein Modell entwickelt, welches sich durch abgrenzbare Phasen auszeichnet.
Als erste Phase des Modells ist die Szenariobeschreibung und –abgrenzung identifiziert worden. Darauf aufbauend lassen sich Bedrohungen, Schwachstellen und Risiken identifizieren. In diesem Aufsatz geschieht dies über Angriffsbäume und Fragenkataloge. Die Quantifizierung der Risiken, sofern möglich, erfolgt über das Value-at-Risk Risikomaß in Verbindung mit einer Monte-Carlo-Simulation. Diese Methode wurde gewählt, da sie neben der leichten Verständlichkeit anschauliche Ergebnisse liefert.
Aufbauend auf der Risikoanalyse lässt sich der Schutzbedarf bestimmen, um in der letzten Phase die geeigneten Schutzmaßnahmen auszuwählen und zu implementieren. Die Aus-

[98] Vgl. Wagner, S. 110.
[99] Rüdiger, S. 6
[100] Vgl. www.trustedshops.de

wahl der Schutzmaßnahmen ist vor allem auf den Schutzbedarf auszurichten, da die Wirtschaftlichkeit der Maßnahmen eine große Rolle spielt. Auch die Akzeptanz der Maßnahmen darf nicht vernachlässigt werden, um sicherzustellen, dass die Maßnahmen insgesamt zu einem positiven Ergebnis führen und ruinöse Schäden vermieden werden.

Die Anwendung des Referenzmodells und Excel-Tools an den Fallbeispielen, zeigt die gute Einsetzbarkeit des Modells in vielfältigen Situationen. Allerdings ist zu beachten, dass durch den Charakter eines Fragenkatalogs nur bereits bekannte Bedrohungen, Schwachstellen und Schutzmaßnahmen zur Verfügung stehen. Deshalb ist eine ständige Weiterentwicklung und Erweiterung der Fragenkataloge notwendig.

Des Weiteren wurde deutlich, dass die Quantifizierung der Risiken teilweise nur sehr schwer möglich ist, da manche Risiken nicht zu quantifizieren sind, z.B. Menschenleben. Zertifizierungen und Gütesiegel sind erforderlich, um die Vergleichbarkeit der Sicherheitskonzepte zu gewährleisten, die Objektivität zu erhöhen und das Vertrauen in die Systeme zu stärken. Durch die Ergebnisse der Experteninterviews wurde deutlich, dass auch andere Wissenschaften das Modell als Grundlage akzeptieren. Allerdings wurde angemerkt, dass sich die Ingenieurwissenschaften naturgemäß vor allem auf die technische Umsetzung der Schutzmaßnahmen konzentrieren.

Schlussendlich ist zu bemerken, dass das Referenzmodell nicht als final zu betrachten ist. Es muss vielmehr als ein wiederkehrender Kreislauf verstanden werden, da auch die Umwelt sich fortlaufend ändert und weiterentwickelt. Ständig entstehen durch den technischen Fortschritt neue Bedrohungen und lassen Schwachstellen relevant werden, die vorher als nicht bedeutsam eingestuft worden sind. Auch werden durch die Weiterentwicklung neue Schutzmaßnahmen möglich, die wiederum andere obsolet werden lassen.

7. Literaturverzeichnis

1. Alexander, C. (2003a): Managing Operational Risks with Bayesian Networks. In: Alexander, C.: Operational Risk; Regulation, Analysis and Management. London et al., S. 285-295, 2003.
2. Basler Ausschuss für Bankenaufsicht : Internationale Konvergenz der Eigenkapitalmessung und der Eigenkapitalanforderungen. http://www.bis.org/publ/bcbs107ger.pdf, abgerufen am 10.12.2008.
3. BITKOM: Kompass der IT-Sicherheitsstandards: Leitfaden und Nachschlagewerk, 2007, http://www.bitkom.org/files/documents/Kompass_der_IT_Sicherheitstandards_final_12_11_2007.pdf, abgerufen am 05.12.2008.
4. Bundesamt für Sicherheit in der Informationstechnik (BSI (A)): http://www.bsi.bund.de/gshb/deutsch/hilfmi/check/04pc_f.pdf, abgerufen am 12.11.2008.
5. Bundesministerium für Sicherheit in der Informationstechnik(BSI (B)): Fragenkatalog Organisation - Revision Stufe 3 http://www.bsi.de/gshb/deutsch/hilfmi/archiv/24_org3.pdf, abgerufen am 10.11.2008.
6. Bundesamt für Sicherheit in der Informationstechnik (BSI (C)): G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen, http://www.bsi.de/gshb/deutsch/g/g03003.htm, abgerufen am 20.10. 2008.
7. Chavez-Demoulin, V./ Embrechts, P.: Advanced extremal models for operational risk. http://www.math.ethz.ch/%7Ebaltes/ftp/opriskevt.pdf, abgerufen am 25.10.2008.
8. Cruz, M.G.: Modeling, Measuring and Hedging Operational Risk. Chichester, 2003.
9. Faisst, U. / Kovacs, M.: Quantifizierung operationelle Risiken - Ein Methodenvergleich. In: Die Bank, Heft 5, S. 342-349, 2003.
10. Geiger, W. / Kotte, W.: Handbuch Qualität. Wiesbaden, 2008.
11. Haubenstock, M. / Hardin, L.: The Loss Distrubution Approach. In: Alexander, C.: Operational Risk: Regulation, Analysis and Management. London et al., S. 171-190, 2003.
12. Hölscher, R. / Kalhöfer, C. / Bonn, R.: Die Bewertung operationeller Risiken in Kreditinstituten. In: FINANZ BETRIEB, Heft 7-8, S. 490-504, 2005.

13. ISO 27001 Security: http://www.27001-online.com, abgerufen am 10.12.2008.
14. IT-Lexikon: http://www.itwissen.info/definition/lexikon/Bedrohung-threat.html, abgerufen am 30.09.2008.
15. Kersten, H., / Reuter, J., / Schröder, K.W.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz – Der Weg zur Zertifizierung. Wiesbaden, 2008.
16. Königs, H.-P.: IT-Risikomanagement mit System. Wiesbaden, 2006.
17. Lassmann, W.: Wirtschaftsinformatik – Nachschlagewerk für Studium und Praxis. Wiesbaden, 2006.
18. Laudon, K.C., Laudon, J.P., Schoder, D.: Wirtschaftsinformatik – Eine Einführung. München, 2006.
19. Meyers Lexikon: Öffentlicher Raum. http://lexikon.meyers.de/wissen/öffentlicher+Raum, abgerufen am 30.09.2008.
20. Müller, K.-R.: IT-Sicherheit mit System – Sicherheitspyramide – Sicherheits-, Kontinuitäts- und Risikomanagement – Normen und Practices – SOA und Softwareentwicklung. Wiesbaden, 2008.
21. Oehler, A. / Unser, M.: Finanzwirtschaftliches Risikomanagement. Berlin, 2002.
22. Piaz, J.-M.: Operational Risk Management bei Banken. Zürich, 2002.
23. Pohlmann, N.: Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen? In Kosten & Nutzen von IT-Sicherheit Heft 248, S. 26-34, 2006.
24. Pohlmann, N. / Blumberg, H.F.: Der IT-Sicherheitsleitfaden. Bonn, 2004.
25. Prokein, O.: IT-Risikomanagement – Identifikation, Quantifizierung und wirtschaftliche Steuerung. Wiesbaden, 2008.
26. Raepple, M.: Sicherheitskonzepte für das Internet – Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung. Heidelberg, 2001.
27. Rau-Medrow, H.: Value at Risk, Expected Shortfall, and Marginal Risk Contribution. 2002, http://www.bwl.uni-wuerzburg.de/fileadmin/12020000/_temp_/Value.pdf, abgerufen am 05.10.2008.
28. Romeike, F.: Risikoidentifikation und Risikokategorien. In: Romeike, F. / Finke, R. B.: Erfolgsfaktor Risiko-Management. Wiesbaden, S. 165-180, 2004.
29. Rommelfanger, H.: Stand der Wissenschaft bei der Aggregation von Risiken, in: Risikoaggregation in der Praxis, Heidelberg, S.15-47, 2008.
30. Rüdiger, K.: Internet-Gütesiegel in Spanien. In: Datenschutz und Datensicherheit, Volume 31 Nummer 6,. Wiesbaden, S.416-421, 2007.
31. Schadt, D.: Über die Ökonomie der IT-Sicherheit. In Kosten & Nutzen von IT-Sicherheit Heft 248, S. 16-25, 2006.
32. Schmid, F., Trede, M.: Finanzmarktstatistik. Heidelberg, 2006.
33. Schmidt, K.: Der IT-Security-Manager. München, 2006.
34. Schneier, B.: Secret & Lies: IT-Sicherheit in der vernetzten Welt. Heidelberg, 2001.
35. Seibold, H.: IT-Risikomanagement. München, 2006.
36. Trusted Shops: Anlage TS-QAL. http://www.trustedshops.de/shopbetreiber/pdf_download/TS-QAL.pdf , abgerufen am 05.12.2008.
37. Vaughan, E.J.: Risk Management. New York, 1997.
38. Wagner, K.W.: PQM – Prozessorientiertes Qualitätsmanagement: Leitfaden der ISO 9001:2000. München, 2003.
39. Wikipedia Enzyklopädie: FMEA. http://de.wikipedia.org/wiki/FMEA, abgerufen am 11.12.2008.
40. Witt, B.C.: IT-Sicherheit kompakt und verständlich: Eine praxisorientierte Einführung. Wiesbaden, 2006.

IWI Discussion Paper Series/Diskussionsbeiträge

ISSN 1612-3646

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IWI Discussion Paper Series/Diskussionsbeiträge

ISSN 1612-3646

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

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

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

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

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

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

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

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

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