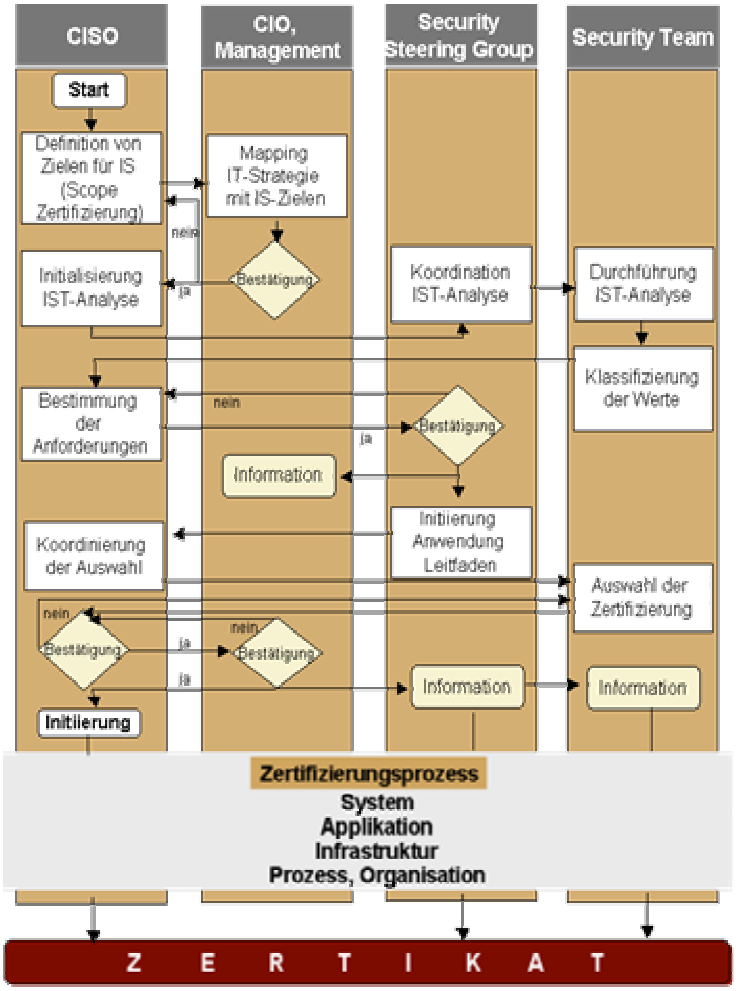
IWI Diskussionsbeiträge

 # 10 (5. Juli, 2004)[1]

ISSN 1612-3646

Mit Zertifizierungen in eine sicherere Informationsgesellschaft[2]

Caroline Neufert[3] und **Michael H. Breitner**[4]



[1] Ausdrucke oder eine PDF-Datei sind auf Anfrage erhältlich: Institut für Wirtschaftsinformatik, Universität Hannover, Königsworther Platz 1, 30167 Hannover, http://www.iwi.uni-hannover.de.

[2] Dieser Aufsatz ist eingereicht für die „7. Internationale Tagung Wirtschaftsinformatik 2005", 23. – 25.2.2005, in Bamberg, vgl. http://www.wi2005.de.

[3] Diplom-Wirtschaftsinformatikerin (FH), M.A. (caroline.neufert@bearingpoint.com).

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

Inhaltsverzeichnis

Mit Zertifizierungen in eine sicherere Informationsgesellschaft

„…people need to be able to trust the systems. This is why security is becoming such an important issue…, we should strive towards a "culture of security"" [Liik04]

Caroline Neufert
BearingPoint GmbH, Berlin

Michael H. Breitner
Universität Hannover

Zusammenfassung: In einer Zeit der zunehmenden Globalisierung der Märkte gewinnen Zertifikate (Gütesiegel) immer stärker an Bedeutung, da sie über Grenzen hinweg den Kunden Vergleich- und Messbarkeit von Produkten bzw. Lösungen, z. B. durch Bestätigung der Einhaltung von Qualitätskriterien ermöglichen. Zertifizierungen sind somit auch ein wirksames Kundenbindungsinstrument. Zertifizierungen auf dem Gebiet der Informationssicherheit stellen nicht nur Messbarkeit her, sondern sichern zugleich die Umsetzung und Einhaltung von notwendigen Maßnahmen, um Informationen ausreichend zu schützen und Vertrauenswürdigkeit in die Leistungsfähigkeit eines Unternehmens herzustellen. Trotz der enormen Tragweite der Evaluation von Zertifizierungen in der Informationssicherheit sind diese Evaluationen von der Wissenschaft bislang weitgehend unbeachtet geblieben. Anhand eines ausgewählten Vorgehensmodells werden System- und Organisationszertifizierungen mit internationaler Anwendbarkeit evaluiert, um Organisationen einen Leitfaden in die Hand zu geben, mit dem sie die für sie optimale Zertifizierung auswählen können.

Schlüsselworte: Informationssicherheit, System- und Organisationszertifizierung, Nutzen einer Zertifizierung, Kundenzufriedenheit, Evaluation, Vorgehensmodell

1 Einleitung und Motivation

In der heutigen, global verbundenen und komplexen Welt ist die Bedeutsamkeit von Informationen und Daten eminent. Mit dem steigenden Gewicht von Informationen und Daten für Unternehmen, Behörden und anderen Organisationen (nach-

folgend unter Organisation subsumiert) wachsen gleichermaßen die Erwartungen und Anforderungen an die Sicherheit dieser Informationen und Daten.

Einer der Schlüsselfaktoren, die Wachstum und Reife einer Organisation darstellen, ist die Informationstechnologie (IT). IT und die von ihr verarbeiteten Informationen sind immer stärker in die Kernprozesse zur Erstellung von Gütern und Dienstleistungen der Organisationen integriert, so dass ein Ausfall der Systeme und Informationen zu entscheidenden, geschäftskritischen Verlusten führen kann, das heißt, dass sich die Risiken und Bedrohungen für die Organisationen permanent erhöhen und gleichzeitig die Kosten für die Begrenzung und Reduktion der Risiken und Bedrohungen steigen.

Die Bedeutung des Schutzes der Informationssysteme und der Informationen steht sowohl aufgrund dieser stärkeren Verzahnung mit den Kernprozessen als auch wegen der erhöhten Forderung nach Transparenz (z. B. Sarbanes-Oxley-Act[1], KonTraG) über die Sicherheit der verarbeiteten Informationen ganz oben auf der Prioritätenliste. Umfassende und ausreichende Maßnahmen sind allerdings selten und meist nicht effektiv implementiert. Verantwortlich dafür sind die unzureichende Kenntnis notwendiger und sinnvoller Maßnahmen in den IT-Abteilungen, mangelndes Commitment des Managements der Organisationen, aber auch die oft in den Raum gestellte Frage der Nutzenbewertung umgesetzter Sicherheitsmaßnahmen. Gerade das Management jedoch muss sich der Frage nach dem Nutzen von Sicherheitsmaßnahmen stellen, um die bei der Umsetzung entstehenden Kosten rechtfertigen zu können.

Zertifizierungen in der Informationssicherheit für Systeme und Organisationen können **das probate Mittel** zur Herstellung und nachhaltigen Verbesserung der Sicherheit sein.

Einerseits geben Zertifizierungen die Gewissheit, innerhalb von Organisationen ausreichende Maßnahmen zum Schutz der Informationen getroffen zu haben und andererseits führen sie den Nachweis nach außen, dem Kunden, Lieferanten, Shareholder etc. gegenüber, eine qualitätsgerechte Verarbeitung ihrer Information gewährleistet und dadurch deren Vertrauen gerechtfertigt zu haben.
In einer Zeit der zunehmenden Globalisierung der Märkte gewinnen international anerkannte Zertifikate oder Gütesiegel immer stärker an Bedeutung, da sie über Grenzen hinweg den Kunden eine Vergleich- und Messbarkeit von Produkten und Lösungen z. B. durch Bestätigung der Einhaltung von Qualitätskriterien ermöglichen. Zertifizierungen sind damit auch ein wirksames Kundenbindungsinstrument. Zertifizierungen auf dem Gebiet der Informationssicherheit stellen hier nicht nur Messbarkeit her, sondern sichern auch die Umsetzung von notwendigen Maßnahmen zu, um die Informationen ausreichend zu schützen und Vertrauenswürdigkeit in die Leistungsfähigkeit des Unternehmens herzustellen. Evaluation und Vergleich von Zertifizierungen in der Informationssicherheit sind aber von der Wissenschaft bislang weitgehend unbeachtet geblieben.

[1]Sarbanes-Oxley-Act: http://www.sarbanes-oxley.com/.

Der vorliegende Aufsatz will sich dieser vernachlässigten Problematik annehmen und sich eingehend mit der Evaluation und dem Vergleich von Zertifizierungen in der Informationssicherheit auseinandersetzen. Nach einigen Begriffserläuterungen wird der Evaluierungsprozess dargestellt, der sich auf Organisationszertifizierungen beschränkt, da diese in ihrer Kosten- und Nutzenbetrachtung wissenschaftlich noch nicht untersucht wurden. Nach der Bewertung der Zertifizierungen wird im nächsten Abschnitt die Umsetzung der Ergebnisse beschrieben. In der Zusammenfassung wird explizit auch auf die Nutzenaspekte eingegangen.

2 Begriffe

2.1 Informationssicherheit

2.1.1 Definition Informationssicherheit

Unter Informationssicherheit wird der Sammelbegriff aller Aspekte zum Schutz von Informationen vor Verlust (Verfügbarkeit), unbefugter Veränderung (Integrität) und unbefugter Kenntnisnahme (Vertraulichkeit) verstanden[2].

2.1.2 Ziele und Grundwerte in der Informationssicherheit

Primäre Ziele und Grundwerte sind:

- **Vertraulichkeit:**

  Informationen, Daten und IT-Systeme dürfen ausschließlich autorisierten Personen oder IT-Prozessen zugänglich sein, d. h. Schutz vor unbefugtem Informationsgewinn muß sichergestellt werden. Beispiele für Maßnahmen: Verschlüsselung, Zugriffsrechte und Passwörter.

- **Verfügbarkeit:**

  Informationen, Daten und IT-Systeme müssen in der erforderlichen Menge und Qualität mit a priori fest vereinbarten Antwortzeiten zur Verfügung stehen. Beispiele für Maßnahmen: Daten-Backup, Disaster Recovery und Archivierung.

- **Integrität:**

  Informationen, Daten dürfen ausschließlich von autorisierten IT-Prozessen oder befugten Personen verarbeitet, z. B. geändert und gelöscht werden. Beispiele für Maßnahmen: Hash-Verfahren und Plausibilitätskontrolle.

[2] British Standard Institute, vgl. http://www.bsi-global.com.

5 Fazit

Organisationen sind heutzutage mehr denn je abhängig von der Informationstechnologie und damit auch stärker von Ausfall und Missbrauch der IT bedroht. Weil die Gefahren so groß und vielschichtig sind, sind Konzepte zum Schutz der IT in aller Munde. Viele Organisationen haben bereits erkannt, dass Informationssicherheit eine ganzheitliche, in der Organisationskultur verankerte Aufgabe des Managements ist.
Ein Allheilmittel zur vollkommenen Sicherheit in der Informationsgesellschaft gibt es nicht! Zertifizierungen jedoch können für Organisationen **das probate Mittel** sein, um die Umsetzung und nachhaltige Einhaltung von Informationssicherheitsmaßnahmen zu dokumentieren und den Kunden, Geschäftspartnern, Shareholdern usw. die Vertrauenswürdigkeit in die eigene Organisation zu beweisen.[18] Die Erhöhung der Kundenzufriedenheit ist sowohl für die bereits bestehende Geschäftsabwicklung als auch für das Neugeschäft nicht zu unterschätzen.

Ungeachtet aller Vorteile, die eine Organisationszertifizierung in der Informationssicherheit bietet, hat sie auch ihren Preis. Es sind finanzielle und personelle Ressourcen erforderlich, die, um auch die Nachhaltigkeit der umgesetzten Maßnahmen zu sichern, nicht nur einmal budgetiert, sondern permanent fortlaufend geplant und bereitgestellt werden müssen.

Trotz der Wichtigkeit sind Zertifizierungen noch kein boomendes Forschungsfeld, was anhand des vorliegenden Aufsatzes thematisiert wird. Gleichzeitig will dieser Aufsatz transparent die Bedeutung von Zertifizierungen in der Informationssicherheit und deren Anwendung darstellen. Es wird ein Lösungsweg aufgezeigt, der global agierenden Organisationen das notwendige Rüstzeug zur Verringerung, Verlagerung, Akzeptanz und/oder Beseitigung der Risiken und Bedrohungen, die durch die immer stärkere Nutzung der Informationstechnologie entstehen, liefert. Dieser Lösungsweg hilft zusätzlich den Organisationen beim Erreichen von Governance, Vertrauen und Zufriedenheit ihrer Partner.

Literatur

[Azar03] Azari, R.: Current Security Management & Ethical Issues of Information Technology, IRM Press, 2003.

[BSI03] Bundesamt für Informationstechnik (BSI): Leitfaden, 2003, http://www.bsi.de.

[18] Nachhaltigkeitsrat: http://www.nachhaltigkeitsrat.de/.

IWI Discussion Paper Series

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 and Michael H. Breitner, *Preisvergleichsdienste: Alternative Konzepte und Geschäftsmodelle*, 22 p., # 3, February 14, 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 and Michael H. Breitner, *Nutzenanalyse im Rahmen der Evaluation von E-Learning Szenarien*, 14 p., #6, October 21, 2003.

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

Heiko Genath, Tobias Brüggemann and Michael H. Breitner, *Preisvergleichsdienste im internationalen Vergleich*, 40 p., #8, June 21, 2004.

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

Caroline Neufert and Michael H. Breitner, *Mit Zertifizierungen in eine sicherere Informationsgesellschaft*, 19 p., #10, July 5, 2004.