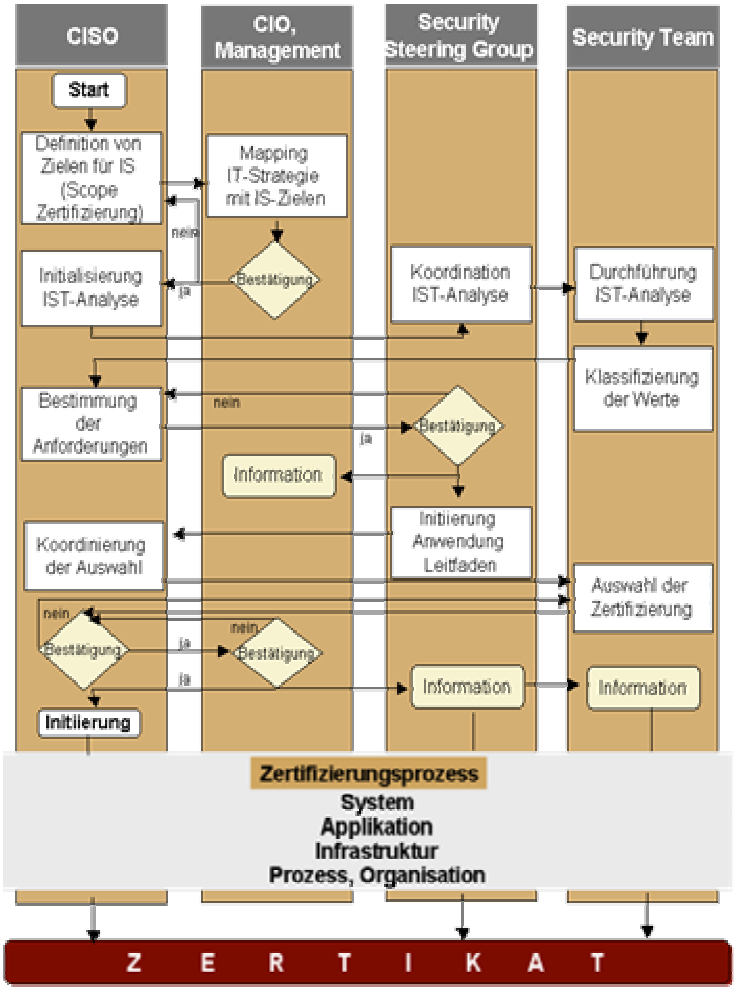
IWI Diskussionsbeiträge

 # 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.

Neben den primären Zielen und Grundwerten gibt es weitere Ziele und Grundwerte:

- **Authentisierung**

  Kommunikationspartner müssen sich zweifelsfrei gegenseitig identifizieren können. Gespeicherte Daten haben einen eindeutigen Ursprung bzw. Besitzer. Beispiele für Maßnahmen: Passwort, Token und Kerberos.

- **Autorisierung**

  Zugriffsrechte auf Informationen, Daten und Diensten müssen an Benutzer zugewiesen und regelmäßig überprüft werden. Beispiele für Maßnahmen: ACL und Single-Sign-On

- **Datenschutz**

  Datenschutz bezweckt den Schutz der Persönlichkeit vor widerrechtlicher oder unverhältnismäßiger Bearbeitung von Personendaten und das Recht auf informationelle Selbstbestimmung [Dwo^{+}00][3]. Die Transparenz und Kontrollierbarkeit soll für die Betroffenen und für unabhängige Kontrollinstanzen, z. B. Datenschutzbeauftragte, gewährleistet sein.

- **Verbindlichkeit**

  Geschäftstransaktionen müssen bestimmten Prozessen und bzw. oder Personen beweissicher zugeordnet werden können. Bei Kommunikationsverbindungen muss die Identität der beteiligten Kommunikationspartner stets bekannt und gesichert sein. Beispiel für eine Maßnahme: elektronische Signatur

2.1.3 Bedrohungen, Risiken und Maßnahmen für die Informationen in Organisationen

Informationen und informationsverarbeitende Prozesse können gefährdet sein durch:

- unbewusstes Fehlverhalten,
- vorsätzliches Handeln,
- technisches Versagen und
- höhere Gewalt.

Der Großteil der Gefahren ist innerhalb von Organisationen zu finden. Risiken von außen drohen u. a. durch:

- ehemalige Mitarbeiter,
- Wirtschaftskriminalität und

[3] BVG zum Volkszählungsurteil, 15.12.1983, http://www.datenschutz.de.

- Hacker.

Verursachte Schäden bzw. Konsequenzen:

- Imageverlust,
- Vertrauensverlust,
- finanzielle Verluste,
- Rechtsbruch, Schadensersatz, Verletzung der persönlichen Selbstbestimmung und der körperlichen Unversehrtheit sowie Störungen der Supply Chain und Störungen in der Kontinuität der Geschäftsprozesse.

2.2 Zertifizierungen

2.2.1 Definition Zertifizierung

Eine Zertifizierung ist das Überprüfen von Organisationen, Systemen, Prozessen, Personen oder Produkten auf die Erfüllung bestimmter Kriterien. Der Nachweis einer Zertifizierung wird durch ein Zertifikat oder Gütesiegel erbracht.

2.2.2 Zertifizierungen in der Informationssicherheit

Zertifizierungen in der Informationssicherheit prüfen und bewerten Produkte bzw. Lösungen, Personen oder Organisationen nach einheitlichen Kriterien. Zertifizierungen in der Informationssicherheit beruhen auf Standards, Methoden oder Best-practice-Ansätzen. Beispielhaft werden nachstehend einige Zertifizierungen kurz beschrieben, vgl. auch [BSI04] und [D21,01].

1. Zertifizierung von Produkten und Lösungen

Unter Produkt bzw. Lösungszertifizierung sind Zertifizierungen zu verstehen, die als Evaluierungsgegenstand[4] ein Produkt/Lösung untersuchen wie:

- **Common Criteria, ISO/IEC 15408** [5]
  Die "Common Criteria for Information Technology Security Evaluation" entstanden 1999 aus einer Fortschreibung von TCSEC (Trusted Computer System Evaluation Criteria) und ITSEC (Information Technology Security Evaluation Criteria). Die Common Criteria bestehen aus mehreren Evaluie-

[4] GI (FG EZQN): http://www.gi-fb-sicherheit.de/fg/ezqn/index.html.
[5] Common Criteria (CC): http://www.commoncriteriaportal.org/.

rungsstufen für Vertrauenswürdigkeit, auf denen Produkte bewertet werden. Innerhalb der Common Criteria werden diese Stufen als Evaluation Assurance Level (EAL) bezeichnet. Dabei ist EAL-1 die niedrigste und EAL-7 die höchste Stufe der Vertrauenswürdigkeit.

- **ISIS-MTT**

  ISIS-MTTv.1.1[6] ist eine gemeinsame Spezifikation des Vereins zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik TeleTrusT und der T7-Gruppe (Die Gruppe besteht aus sieben in Deutschland ansässigen Trustcentern) für elektronische Signaturen, Verschlüsselung und Public-Key-Infrastrukturen. Die Industrial Signature Interoperability and Mailtrust Specification beinhaltet Part 1: Certificate and CRL Profiles, Part 2: PKI Management, Part 3: Message Formats, Part 4: Operational Protocols, Part 5: Certificate Path Validation, Part 6: Cryptographic Algorithms, Part 7: Cryptographic Token Interface und Part 8: XML Signature and Encryption Message Formats.

- **FIPS 140-2** [7]

  Der Federal Information Processing Standards wurde von dem National Institute of Standards and Technology (NIST) erarbeitet und legt Sicherheitskriterien für kryptographische Module fest. Der Standard nutzt vier Sicherheitslevels, die alle potentiellen Applikationen und Umgebungen, die kryptographische Module einsetzen, bewerten und untersuchen. Das Cryptographic Module Validation Program (CMVP) validiert diese Module gemäß FIPS 140-2 nach dem Test in akkreditierten Testlabors.

2. Personen

Zertifizierungen für Personen belegen deren Kenntnis und Wissen auf dem Gebiet der Informationssicherheit.

- **CISSP** [8]

  Die Prüfung zum Certified Information Systems Security Professional (CISSP) deckt sämtliche Gebiete der Informationssicherheit ab, d. h. Bestandteil sind die Gebiete:
  - Zugriffskontrollsysteme und Methodologie,
  - Telekommunikations- und Netzwerksicherheit,
  - Praxis des Sicherheitsmanagements,
  - Anwendungs- und Systementwicklung,

---

[6] ISIS-MTT: Industrial Signature Interoperability and Mailtrust Specification v1.1: http://www.isis-mtt.org oder http://www.t7-isis.de.

[7] FIPS 140-2: Federal Information Processing Standards: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[8] $(ISC)^2$: International Information Systems Security Certification Consortium: http://www.isc2.org/.

- Kryptographie,
- Sicherheitsarchitekturen und –Modelle,
- Betriebssicherheit und Operating,
- Kontinuitätsmanagement und Notfallplanung,
- rechtliche und ethische Aspekte und
- physische Sicherheit.

Die Zertifizierung wird von einem weltweit tätigen, nicht-profit-orientierten International Information Systems Security Certification Consortium (ISC)[2] vergeben.

- **CISA** [9]

  Der Certified Information Systems Auditor ist ein Zertifikat im Bereich der Revision, Kontrolle und Sicherheit von Informationssystemen. Es wird von der ISACA verliehen. Wichtige Voraussetzung zur Erlangung des Zertifikats ist - neben einer mehrjährigen Berufserfahrung - das Bestehen der CISA-Prüfung. Die Prüfungsanforderungen werden ständig an die fortlaufende Entwicklung der Informationstechnologien bzw. der Tätigkeit eines Spezialisten im Bereich der Revision, Kontrolle und Sicherheit der Informationstechnologie angepasst.

- **CompTIA Security+** [10]

  Computing Technology Industry Association ist ein Non-Profit-Zusammenschluss der IT-Branche mit derzeit 19000 Mitgliedern, um Industrie-Standards und IT-Expertise zu fördern. CompTIA Security+ testet Security Wissen auf den Gebieten Netzwerk, Kommunikationssicherheit, Infrastruktur, Kryptographie, Zugangskontrolle, Authentifizierung und Organisationssicherheit.

3. Organisation

Organisationszertifizierungen haben als Evaluierungsgegenstand komplexe IT-Systeme, Abteilungen, regionale Niederlassungen oder das gesamte Unternehmen.

- **IT-Grundschutzhandbuch** [11]
  Ziel des IT-Grundschutzes ist es, durch infrastrukturelle, organisatorische, personelle und technische Standard-Sicherheitsmaßnahmen ein Standard-Sicherheitsniveau aufzubauen, das aufgrund seiner Modularität ausbaufähig ist [BSI]. Dafür schlägt das IT-Grundschutzhandbuch Standard-Sicherheitsmaßnahmen aus den Bereichen Infrastruktur, Organisation, Perso-

[9] ISACA: Information Systems Audit and Control Association: http://www.isaca.org/.
[10] CompTIA: Computing Technology Industry Association: http://www.comptia.org/certification/security/default.asp.
[11] Bundesamt für Informationstechnik (BSI): http://www.bsi.de.

nal, Hard- und Software, Kommunikation und Notfallvorsorge vor. Die Vorgehensweise umfasst die Arbeitsschritte IT-Strukturanalyse, Schutzbedarfsfeststellung, Risikoanalyse und Realisierung von IT-Sicherheitsmaßnahmen[D21,01].

- **ISO / IEC 17799 und BS 7799** [12]
  Ziel der ISO/IEC 17799 (BS 7799) ist es, ein Managementsystem aufzubauen, das umfassende Maßnahmen bereitstellt, die dem Best-practice-Ansatz in der Informationssicherheit genügen. Der Standard besteht aus zwei Teilen. Teil 1 beschreibt die Maßnahmen, Teil 2 bildet die Basis für die Beurteilung des Informationssicherheits-Managementsystems, die für ein formales Verfahren zur Zertifizierung herangezogen wird.
  Betrachtet werden Aspekte der Sicherheitspolitik, Organisation der Sicherheit, Einstufung und Kontrolle der Werte, personelle Sicherheit, physische und umgebungsbezogene Sicherheit, Management der Kommunikation und des Betriebs, Zugangskontrollen, Systementwicklung und Wartung, Management des kontinuierlichen Geschäftsbetriebs und die Einhaltung von Verpflichtungen.

- **HIPAA** [13]
  1996 wurde das gegenwärtig in den USA für den medizinischen Bereich gültige Gesetzeswerk Health Insurance Portability and Accountability Act in Kraft gesetzt, das u. a. Regelungen zu Datenschutz und Datensicherheit enthält. Um den Anforderungen des Gesetzes zu genügen, sind Maßnahmen zu Zugangskontrolle, Konfigurationsmanagement, Virusprüfung, Incident Management, physische Sicherheit, Rollen, Befugnisse und Verantwortlichkeiten zu implementieren.

2.3 Evaluation

In der Sozialwissenschaft und in der Technik bedeutet der Begriff „Evaluation“ Analyse und Bewertung eines Sachverhalts, die Effizienz- und Erfolgskontrolle einer Innovation, die Beurteilung von Zielen und Maßnahmen einer Planung sowie die Einschätzung von Wirksamkeit und Wirkungszusammenhängen [Broc01]. Für eine Evaluation müssen Informationen und Daten methodisch organisiert erhoben und systematisch dokumentiert werden, um die Untersuchung, das Vorgehen und die Ergebnisse a posteriori nachvollziehbar und überprüfbar zu machen.

[12] British Standard Institute: http://www.bsi-global.com und http://www.iso-17799.com/.
[13] Health Insurance Portability and Accountability Act (HIPAA): http://www.hipaa.org/ und http://www.hhs.gov/ocr/hipaa/.

3 Status quo der Informationssicherheit

Mit der gewachsenen Bedeutung der Informationssicherheit, die essentieller Bestandteil der Kernprozesse ist, sind gleichermaßen - wie aktuelle Analysen beweisen - die Gefahren gestiegen.

Jahr	Vorfälle	Schwachstelle
1990	**252**	**-**
1995	**2.412**	**171**
2000	**21.756**	**1.090**
2001	**52.658**	**2.437**
2002	**82.094**	**4.129**
2003	**137.529**	**3.784**

Tabelle 1: Festgestellte und gemeldete Sicherheitsvorfälle und Schwachstellen von Organisationen. Quelle: http://www.cert.org/stats.

Die gesunkene Zahl der Schwachstellen im Verhältnis zu den stark gestiegenen Vorfällen resultiert auch aus der erkannten Bedeutung der Informationssicherheit in den Organisationen. Anhand eines Auszuges aus einer Studie zu IT-Trends 2004 wird dies deutlich.
In einer Skala von 1 = sehr wichtig bis 6 = unwichtig, n.e. = nicht erhoben steht die Wichtigkeit der Sicherheit im Jahr 2004 an erster Stelle.

	2004	2003	2002
Sicherheit	**1,7**	**n.e**	**n.e**
ERP	**2,48**	**2,83**	**2,6**
EAI	**2,96**	**3,08**	**3,07**
Portale	**3,04**	**2,33**	**2,58**

Tabelle 2: Wichtigkeit von IT-Themen. Quelle: Cap Gemini E&Y, 2004: Studie IT Trends 2004 (Zahl der befragten Organisationen im Durchschnitt 130).

Die nächste Abbildung zeigt aber auch auf, wie das Thema Sicherheit in den Organisationen behandelt wird.

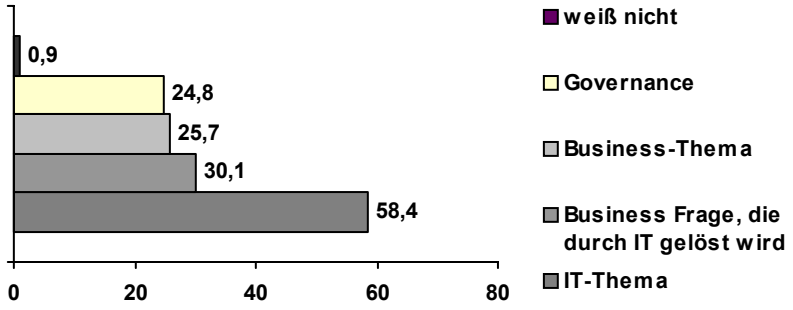


Abbildung 1: Bedeutung und Auffassung von Sicherheit in einer Organisation Quelle: Cap Gemini E&Y, 2004: Studie IT Trends 2004, siehe oben.

Die Organisationen wissen, dass für die permanente Erhaltung der Informationssicherheit etwas getan werden muss. Dass international anerkannte Zertifizierungen für Organisationen auf diesem Gebiet ein probates Mittel sein können, ist jedoch noch nicht von dem für Informationssicherheit verantwortlichen Management erkannt worden, so dass die Zahl der zertifizierten Organisationen auf dem Gebiet der Informationssicherheit noch immer relativ gering ist. Zum einen fehlt es an einer wissenschaftlich fundierten Untersuchung darüber, zum anderen ist der Markt für Zertifizierungen gegenwärtig unübersichtlich und kaum konsolidiert, so dass sich bisher keine Standards durchsetzen konnten, die auf eine breite internationale Akzeptanz stoßen.

Viele Organisationen überlegen zwar, sich zertifizieren zu lassen, scheuen jedoch, da ihnen der Nutzen der jeweiligen Zertifizierung unklar ist, die hohen Kosten. Sie sehen sich noch immer außerstande, eine detaillierte und fundierte Entscheidung zu fällen, welche Zertifizierung für sie sinnvoll ist.

Folgende Faktoren sind dafür meist ausschlaggebend:

- politische Zwänge und die Einhaltung von regionalen Gesetzen,
- finanzielle Möglichkeiten,
- Vielfalt von Zertifikatsangeboten am Markt.

In diesem Zusammenhang muss die Frage beantwortet werden, welche Zertifizierung für Informationssicherheit für welche Organisation optimal ist. Im Einzelnen ist zu entscheiden:

- Wo und unter welchen Bedingungen soll die Zertifizierung zum Einsatz kommen?

- Welche Sicherheitsaussage lässt sich auf Grundlage der einzelnen Kriterienwerke treffen?
- Schließt die Evaluation der Zertifizierungen eine Kosten- und Nutzenanalyse ein?
- Wo liegen angesichts beschränkter Ressourcen die Prioritäten in der Sicherheitspolitik des Unternehmens sowohl in Hinsicht auf die strategischen Geschäftsziele als auch auf die Maßnahmen, die zum Einsatz kommen könnten?
- Liegt die Betonung auf Wahrung oder Weiterentwicklung der Sicherheit in der Organisation?
- Wie wird die Nachhaltigkeit einer Zertifizierung gesichert?

4 Eine optimale Zertifizierung für eine sicherere, vertrauenswürdigere Organisation

Die öffentliche Diskussion um Zertifizierungen in der Informationssicherheit konzentriert sich immer wieder auf regionale Abgrenzungen oder auf das Abbilden verschiedener Standards und Zertifizierungen einer ausgewählten Zertifizierung. Zu kurz kommt eine fundierte Bewertung der einzelnen Kriterien. Damit sind für eine Konkretisierung, d. h. für die Praktikabilität der Ergebnisse und der in Abschnitt 3 gestellten Fragen, die Erkenntnisse oft unzureichend.

Um zur Auswahl der optimalen Zertifizierungen für eine Organisation zu gelangen, müssen sowohl die Kriterien zur Bestimmung erweitert als auch der Referenzwert für die Bewertung der Ziele von Organisationen angepasst werden. Von dieser Evaluation ausgehend wird ein Leitfaden vorgestellt, der die Informationssicherheit ganzheitlich - auch hinsichtlich des Nutzens von Zertifizierungen und nicht nur in Bezug auf die Kosten - betrachtet.

4.1 Evaluierungsprozess

Für die Auswahl der optimalen Zertifizierung von Organisationen auf dem Gebiet der Informationssicherheit ist es notwendig, die am Markt (soweit bekannt) verfügbaren Standards bzw. Zertifizierungen nach Produkten und Lösungen, Personen und Organisationszertifizierungen zu klassifizieren (vgl. hierzu Abschnitt 2). Im nächsten Schritt werden die Kriterien für die Bewertung der einzelnen Zertifizierungen bestimmt. Die Auswahl kann unterstützt werden durch gängige Kennzahlensysteme[14]. Diese Kriterien umfassen unter anderem:

[14] Balance Scorecard: http://www.balancedscorecard.org/.
Six Sigma: http://www.6-sigma.com/.

- Aspekte aus der Informationssicherheit und Informationstechnologie wie Funktionalität und Beurteilungsumfang, Anwendungsgebiete, Detailtiefe der Maßnahmen und Umsetzbarkeit,
- wirtschaftliche Rahmenbedingungen wie Berücksichtigung von betriebswirtschaftlichen Kenngrößen, Investitionsschutz, Innovationsfreudigkeit, Ressourcenbedarf, Vermarktung, Software-Unterstützung,
- regulatorische Rahmenbedingungen wie Einhaltung von Gesetzen, sonstige Aspekte wie Ablauf der Zertifizierung bzw. Rezertifizierung, strategische Ausrichtung der Zertifizierung (Nachhaltigkeit), Unabhängigkeit.

Nach der Bestimmung der Kriterien ist es erforderlich, als nächsten Schritt einen Referenzwert für die Evaluation zu definieren, der transparent, anspruchsvoll, unabhängig, kontinuierlich und glaubhaft ist. Um dieses Ziel zu erreichen, eignet sich besonders gut die Anwendung des Reifegradmodells CMMI[15] [CMMI, Capability Maturity Model Integration], [Kass04], [MuSt03]. Angelehnt an dieses Modell werden die Kriterien in ihrer Umsetzung in Reifegrade unterteilt. Das geschieht in fünf Stufen, von keinen definierten Anforderungen über wohl strukturierten bis hin kontinuierlich nachhaltig verbesserten und angepassten Kriterien. Der Vorteil des Reifegradmodells besteht darin, dass es die Bestimmung von Kriterien unabhängig von der zu untersuchenden Zertifizierung und der Bewertung des Erreichens dieser Kriterien ermöglicht. Darüber hinaus kann dieses Modell die Kriterien in ihrem Zusammenwirken erfassen und somit die Auswirkungen auf Abhängigkeiten bewerten.
Die Evaluation der einzelnen Kriterien für das Ausarbeiten der Auswahl der optimalen Zertifizierung für Organisationen ist kein statischer Prozess. Der iterative und zyklische Prozess der Evaluation der einzelnen Kriterien wird anschaulich anhand des folgenden Modells dargestellt.

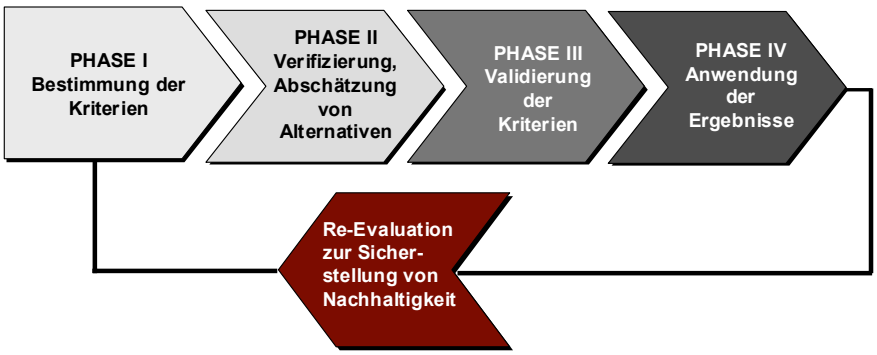


Abbildung 2: Darstellung des Evaluationsprozesses

[15] Capability Maturity Model: http://www.sei.cmu.edu/cmmi/.

Im Folgenden wird das methodische Vorgehen detailliert beschrieben:

- **Phase 1**
  In der Phase 1 werden zuerst die Evaluierungsziele bestimmt. Randbedingungen und Abhängigkeiten, denen die Zertifizierung unterliegt, werden aufgezeigt.
  Die Risiken und Bedrohungen werden aufgelistet. Abhängig von diesen Risiken können alternative Strategien geplant oder die Auswahl der Kriterien angepasst werden. Jede Alternative wird mit jedem Ziel verglichen. Das führt wieder zu einer Bestimmung möglicher Risiken.

- **Phase 2**
  Im nächsten Schritt werden die ermittelten Kriterien verifiziert und einer eingehenden Risikoanalyse unterzogen. Jedes einzelne Kriterium wird dahingehend überprüft, ob es überhaupt anwendbar, messbar und vergleichbar ist. Darüber hinaus werden strukturelle Überprüfungen durchgeführt zur Entdekkung von redundanten Regeln und von logischen Inkonsistenzen.

- **Phase 3**

  Nach der Auswertung der Risiken werden die Ergebnisse validiert, um die Richtigkeit und Zuverlässigkeit der Evaluation zu überprüfen. Die Validierung wird schrittweise durchgeführt, beginnend mit der Beurteilung einzelner Kriterien, dann der Untersuchung von logischen Beziehungen zwischen Kriterien und schließlich einer Überprüfung der gesamten Kriterienauswahl.

- **Phase 4**
  Der gesamte Evaluierungsprozess wird einem Review unterzogen. Bei positivem Ergebnis wird ein Leitfaden erstellt, der Hinweise zur Integration, Realisierung und Nachhaltigkeit der Ergebnisse beinhaltet.

  In der Phase der Re-Evaluation wird in regelmäßigen, zeitlichen Abständen die Nachhaltigkeit der ausgewählten und bewerteten Kriterien überprüft.

Nach Beendigung des Evaluierungsprozesses liegt der jeweiligen Organisation ein Leitfaden vor, mit dem die für die betreffende Organisation optimale Zertifizierung bestimmbar ist. Dieser Leitfaden gibt detailliert und konkret Auskunft zu Themen und Fragestellungen wie:

- Welche Sicherheitsaussage lässt sich auf Grundlage der einzelnen Kriterienwerke treffen?
- Schließt die Evaluation der Zertifizierungen eine Kosten- und Nutzenanalyse ein?
- Wie wird die Nachhaltigkeit einer Zertifizierung gesichert?

4.2 Auswahlprozess

Anhand des Auswahlprozesses sollen folgende Fragen beantwortet werden:

- Wo und unter welchen Bedingungen soll die Zertifizierung zum Einsatz kommen?
- Wo liegen angesichts beschränkter Ressourcen die Prioritäten in der Sicherheitspolitik der Organisationen sowohl in Hinsicht auf die strategischen Geschäftsziele als auch auf die Maßnahmen, die zum Einsatz kommen könnten?
- Liegt die Betonung auf der Wahrung oder der Weiterentwicklung der Sicherheit in der Organisation?

Für die Klärung dieser Fragen ist der Auswahlprozess innerhalb der Organisation entscheidend. Um zu einer fundierten Entscheidungsvorlage für die Auswahl einer Zertifizierung zu gelangen, müssen folgende Einflussfaktoren berücksichtigt werden:

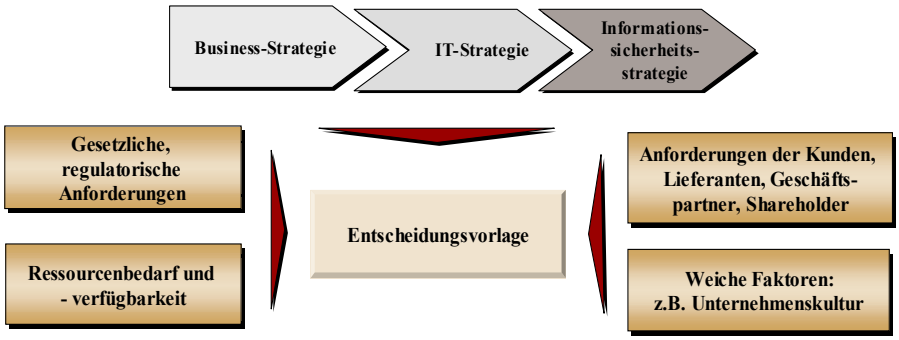


Abbildung 3: Einflussfaktoren für die Entscheidung für eine Zertifizierung

Diese Vorlage bildet mit ihren in der Abbildung gezeigten Einflüssen die Grundlage zur Entscheidung für eine Zertifizierung, die Anwendung des Leitfadens und für die spätere Definition der kritischen Erfolgsfaktoren. Darüber hinaus fließt die Entscheidungsvorlage in bestehende Managementinformationssysteme ein und kann damit auch als Steuerungs- und Controllinginstrument genutzt werden.

Das methodische Vorgehen für die Anwendung des Leitfadens zur Auswahl einer optimalen Zertifizierung zu finden, wird im nachfolgenden Prozessbild verdeutlicht. Involvierte Parteien sind der CISO (Corporate Information Security Officer) als Initiator, der CIO und das Management als Befürworter, die Security Steering Group zur Steuerung und Koordinierung und das Sicherheitsteam mit integriertem CERT (Computer Emergency Response Team) für die Umsetzung der Anforderungen.

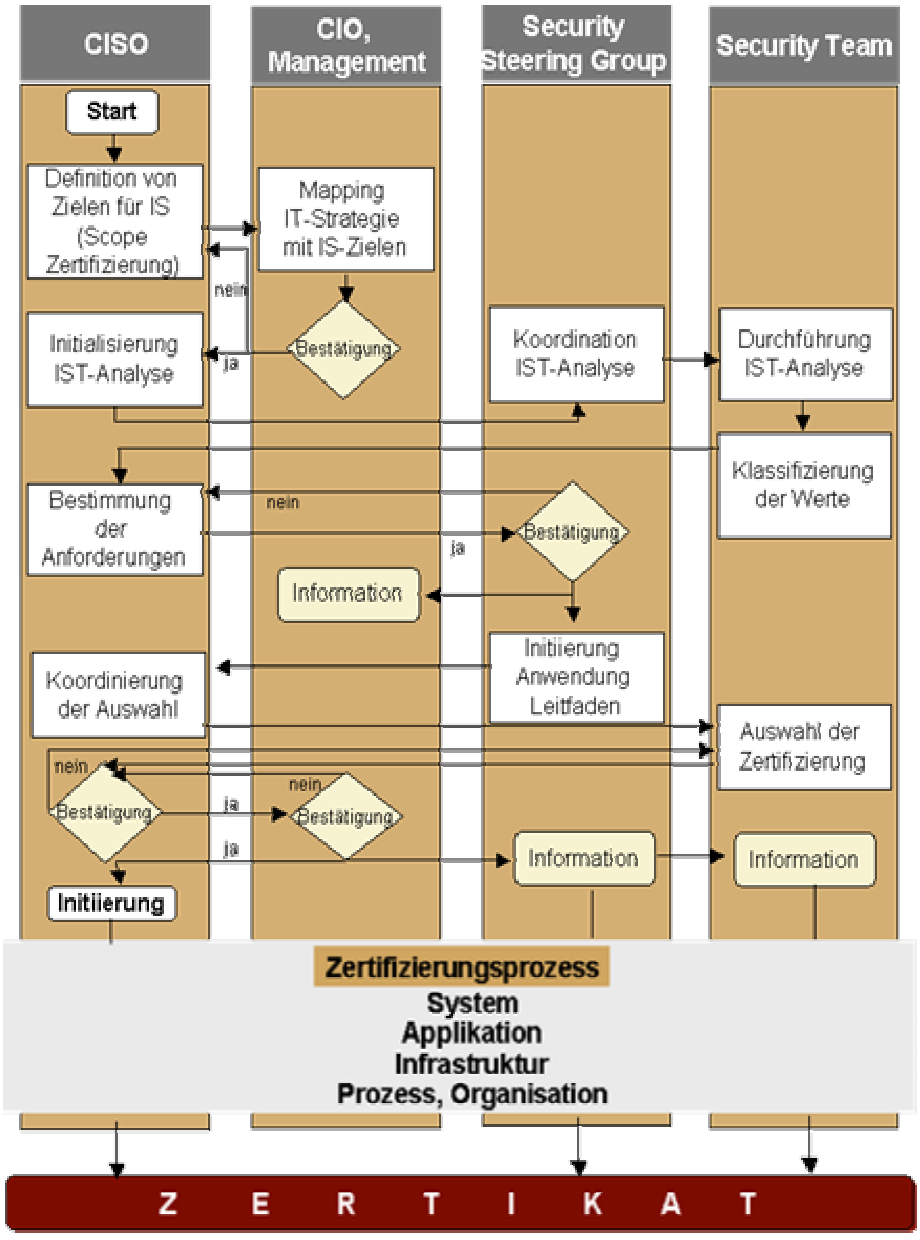


Abbildung 4: Anwendung des Leitfadens

Für die Umsetzung der Maßnahmen, die für die ausgewählte Zertifizierung erforderlich sind, können klassische Projektmanagementmethoden wie das PDCA-Modell (Plan, Do, Check, Act)[16] oder Proven-Course™ (Management von Strategy, Design, Build, Deploy, Operate) [17] in Anspruch genommen werden.

4.3 Nutzen von Zertifizierungen

- Organisationen können ihre Anstrengungen hinsichtlich Informationssicherheit publizieren und diese als wirksames CRM-Instrument unter anderem zur Erhaltung und Steigerung der Kundenzufriedenheit benutzen.
- Anforderungen nationaler und internationaler Gesetze (z. B. Transparenz) werden erfüllt.
- Organisationen sind mit Hilfe eines Zertifikats in der Lage, den vertrauenswürdigen Nachweis zu führen, dass ihr Unternehmen hinsichtlich Informationssicherheit „State of the Art“ ist (z. B. für eine Mitgliedschaft in Netzwerken oder Verbänden, in Lieferantenbeziehungen und Lieferketten und zur Verringerung von Markteintrittsbarrieren).
- Zertifizierungen ermöglichen ein permanentes Monitoring und Benchmarking und sichern Nachhaltigkeit.
- Aufgrund der Liberalisierung der Märkte werden einheitliche, international anerkannte Standards und Normen, die in eine Zertifizierung münden, immer wichtiger, um weltweit konkurrenzfähig zu bleiben.
- Informationssicherheit ist ein Wirtschaftsfaktor durch den Ressourcenbedarf der für die nötigen Maßnahmen zur Erhaltung des Betriebs bereitgestellt werden muss. Mit Hilfe von Zertifizierungen können die Investitionen messbar und bewertbar gemacht werden.

Nach Erhalt eines Zertifikats sind die Vorteile für Organisationen also evident.

[16] IBM: http://www.ibm.com.
[17] BearingPoint Inc.: http://www.bearingpoint.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/.

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

[Dwo+00] Dworatschek, S, Büllesbach, A., Koch, H.-D.: PC & Datenschutz. Datakontext, 2000, S. 38.

[D2101] Initiative D21 (D21): IT-Sicherheitskriterien im Vergleich, 2001, http://www.bsi.de.

[Ecke03] Eckert, C.: IT-Sicherheit, Oldenbourg, 2003.

[Fede02] Federrath, H.: Die bedrohte Sicherheit von Informationsnetzen in Felicitas von Aretin, Bernd Wannenmacher (Hrsg.): Weltlage - Der 11. September, die Politik und die Kulturen, Opladen, 2002.

[FePf02] Federrath, H., Pfitzmann, A.: Sicherheit im Netz, in: Hans-Werner Moritz, Thomas Dreier (Hg.): Rechts-Handbuch zum E-Commerce, Schmidt, 2002.

[Kass04] Kasse, T.: Practical Guide to CMMI, Artech House Publishers, 2004.

[Liik04] Liikanen, E.: Rede auf der CeBIT 2004, Hannover, 18.3.2004.

[MuSt03] Mutafelifa, B., Stromberg, H.: Systematic Process Improvement Using ISO 9001: 2000 and CMMI, Artech House Publishers, 2003.

[PoBl04] Pohlmann, N., Blumberg, H.: Der IT-Sicherheitsleitfaden, Mitp, 2004

[Rann00] Rannenberg, K.: IT Security Certification and Criteria. In Sihan Qing, Jan H.P.Eloff: Information Security for Global Information Infrastructures; Proceedings of the 16th Annual Working Conference on Information Security, 2000, pp. 1-10.

[Schn01] Schneier, B.: Secrets & Lies. IT-Sicherheit in einer vernetzten Welt, Wiley, 2001.

[Wyld03] Wylder, J.: Strategic Information Security, Auerbach Publications, 2003.

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.