Konzepte der Informationssicherheit in Standards am Beispiel ISO 27001

Danijel Milicevic, Matthias Goeken

IT-Governance-Practice-Network, Frankfurt School of Finance & Management
Sonnemannstr. 9-11, 60314 Frankfurt am Main
{ d.milicevic, m.goeken } @ frankfurt-school.de

Die Dynamik der Informationstechnologie und steigende Komplexität von Informationssystemen schlägt sich auch im Informationssicherheitsmanagement nieder. Informationssicherheitsstandards haben sich als generische Lösungen für eine Vielzahl von Aufgaben etabliert. Inwieweit derartige Standards die benötigte ganzheitliche Betrachtung vorsehen ist bislang nicht geklärt. Im vorliegenden Beitrag wird ein Metamodell des ISO 27001 Standards auf Basis einer qualitativen Datenanalyse erstellt, um die betrachteten Konzepte zu identifizieren und einen Einblick in die Kernelemente des Standards zu liefern.

1 Einleitung

Medienwirksame Sicherheitsvorfälle, Bemühungen von Datenschützern und eine verschärfte Gesetzgebung sorgen dafür, dass die Informationssicherheit eins der wichtigsten Themen für CIOs und IT-Manager darstellt. Während in der Vergangenheit der Mangel derartiger Aufmerksamkeit und Unterstützung durch das Management häufig als eins der größten Probleme benannt wurde, ist mittlerweile die steigende Komplexität ein wichtiger Faktor. Hieraus ergibt sich ein Bedarf nach einem umfassenden Sicherheitsmanagement und der Bedarf nach unternehmens- und branchenübergreifenden Richtlinien und Referenzen führte zur Bildung von Informationssicherheitsstandards. Als ein Bündel von sogenannten Best Practices bieten sie eine Übersicht der facettenreichen Informationssicherheitsdomäne. Einige Forscher stehen derartigen Standards kritisch gegenüber. So stellen bspw. [SW09] ihre Validität und inhaltliche Detailtiefe in Frage. Der vorliegende Beitrag beschäftigt sich damit, wie umfassend Informationssicherheitsstandards die Problemdomäne erfassen.

Der Aufbau von Informationssicherheitsmanagementsystemen sollte einen umfassenden oder gar „ganzheitlichen“ Ansatz verfolgen, falls man Effektivität gewährleisten möchte [BW07]. Zum Zweck der Analyse mit Blick auf „Ganzheitlichkeit“ leiten wir Konzepte der Informationssicherheit aus einem prominenten Standard ab und modellieren Sie auf einer Ebene, welche einen Vergleich mit in der Wissenschaft entstandenen Ontologie zulässt (auf Grund von Platzgründen nicht Teil dieses Beitrages). Zuvor werden die Forschungsmethodik und das Vorgehen bei der Metamodellierung erläutert (Teil 2). Das Metamodell des ISO 27001 wird in Teil 4 beschrieben.

2 Forschungsmethodik

In der vorliegenden Arbeit wird eine theoretische Fundierung über semi-formale Modelle der Informationssicherheit angestrebt. Falls der Untersuchungsgegenstand der Modellierung Modelle sind und nicht etwa Realobjekte, so spricht man von Metamodellen. [St96] betrachtet, wie durch Metaisierung Hierarchien von Modellen konstruiert werden. Das Metaisierungsprinzip beschreibt „denjenigen Aspekt eines Modells, der in der übergeordneten Modellierungsstufe abgebildet wird." Sie betont, dass verschiedene Möglichkeiten bestehen, um von den Instanzen der Wirklichkeit zu Modellen und schließlich zu Metamodellen kommt [siehe auch Le05]. Das Metaisierungsprinzip definiert demnach in einer Modellhierarchie den Abstraktionsmechanismus zur Strukturierung der Objekte der jeweils darunterliegenden Ebene. Beispiele sind die linguistische, ontologische und physische Metaisierung. Für eine detaillierte Darstellung sei an dieser Stelle auf [Le05 und GH05] verwiesen. Im Rahmen der vorliegenden Fragestellung ist insbesondere die ontologische Metamodellierung von Bedeutung, bei der die Abstraktion von Modellelementen gemäß ihrem Inhalt stattfindet.

Metamodelle stellen die zugrundeliegende, häufig implizite, Struktur von Modellen dar. Diese Repräsentation kann je nach Motivation verschiedenartig genutzt werden. Zum einen bieten Metamodelle methodische Unterstützung bei der Erweiterung und Veränderung von Modellen. Berücksichtigt man die Struktur eines Modells bei einer derartigen Adaption, ist eine Konformität mit dem ursprünglichen Modell bzw. Standard wahrscheinlicher. Ebenfalls können Metamodelle zur Integration mehrerer Modelle dienen, als auch Grundlage für die Entwicklung einer entsprechenden Werkzeugunterstützung sein. Im vorliegenden Beitrag ist die Motivation analytischer Natur, so dass die Metamodellierung des Standards als Grundlage für eine Analyse und Evaluation der Vollständigkeit durch Vergleich mit einer Sicherheitsontologie genutzt wird. Bei der Erstellung von Modellen, somit auch Metamodellen, bedarf es einer Sprache und einer Methode im Sinne einer Vorgehensweise, die die Identifikation wie auch Repräsentation der relevanten Objekte im Modell unterstützt. Die Sprache bzw. Sprachauswahl wird auch plastisch „way of modeling" bezeichnet, die Vorgehensweise als „way of working" [VHW91]. Hier werden UML-Klassendiagramme verwendet. Im Folgenden soll der „way of working" detaillierter betrachtet werden.

Als methodische Fundierung des Konstruktionsprozesses von Metamodellen findet im vorliegenden Beitrag eine Anlehnung an die Grounded Theory und die qualitative Datenanalyse (QDA) statt. Aufgrund der Seitenbeschränkung soll hier von einer detaillierten Darstellung abgesehen werden und stattdessen auf die relevante Literatur verwiesen werden, wie z.B. [CS90, Gr95]. Die grundlegende Idee der Grounded Theory ist das Arbeiten mit empirischen Daten wie die Transkription von Interviews, Protokolle und Dokumente, mit welchen der Forscher im Feld konfrontiert ist. Der Fokus liegt dabei auf dem induktiven Generieren von Theorien, welche in den jeweiligen empirischen Daten „verankert" (grounded) sind. Eine zentrale Aktivität in der qualitativen Datenanalyse stellt dabei die Kodierung dar. Kodierung bedeutet hierbei die Konzeptualisierung von Daten und Herleitung von Kategorien, sowie Beziehungen zwischen ihnen. Die in den Daten gefundenen Ereignisse und Instanzen werden

analysiert als potentielle „indicators of phenomena … which are thereby given conceptual labels“ [CS90, p. 7]. Diese Konzeptualisierung ist der vorab beschriebenen ontologischen Metaisierung sehr ähnlich. Im Folgenden wird ein Informationssicherheitsstandard als Ursprungsdokument verwendet und mittels induktiver Kategorisierung in ein Metamodell überführt.

3 Informationssicherheitsstandards

Eine der größten Herausforderungen im Informationssicherheitsmanagement sind unvollständige Informationen über die Risiken, denen Informationssysteme ausgesetzt sind sowie Gegenmaßnahmen. Dies begründet unter anderem die Popularität von Planungsmodellen, Checklisten und Richtlinien als Referenzen im Informationssicherheitsmanagement. Während einzelne Unternehmen Bedrohungen gegenüber ihren Informationssystemen identifizieren und Gegenmaßnahmen abwägen und implementieren, kristallisieren sich erfolgreiche Aktivitäten und Prozesse heraus (Best Practices). Im Rahmen von Standardisierungsbemühungen durch sog. Standard-Setter fließen derartige Best Practices in erste Entwürfe für neue Standards ein. Diese haben selbst im Rahmen der Informationssicherheit unterschiedliche Foki und Ausrichtungen. Bei der Auswahl eines Informationssicherheitsstandards wurden zwei Anforderungen formuliert: 1) der Standard muss eine umfassende und breite Betrachtung der Informationssicherheit als Ziel haben und 2) er sollte - wenn auch beschränkt - eine gewisse Repräsentativität für den tatsächlichen Umgang mit Informationssicherheit in der Praxis darstellen.

Nach einer Evaluation mehrerer Standards fiel die Wahl auf ISO 27001 [In05]. Der ISO-27002-Standard, welcher die eigentliche Best-Practices-Richtlinie für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS) ist, wird in der Regel nicht vollständig adaptiert [LG10]. Der ISO-27001-Standard hingegen ist ein Zertifizierungsstandard. Dadurch ist gewährleistet, dass zertifizierte Unternehmen ihn in Gänze implementiert haben (ggf. mit Erweiterungen). Dies bedeutet im Umkehrschluss, dass der Zertifizierungsstandard, zumindest für zertifizierte Unternehmen, die tatsächliche Praxis im Informationssicherheitsmanagement darstellt.

4 Metamodellierung von ISO 27001

Durch die Wahl des ISO-27001-Zertifizierungsstandards als Untersuchungsgegenstand ist das Primärdokument bereits bestimmt. Als Primärdokument wird im verwendeten Atlas.ti-Werkzeug das zu kodierende Dokument bezeichnet. Eine weitere Eingrenzung findet dadurch statt, dass lediglich der Anhang A „Control objectives and controls“ aus dem Standard kodiert werden soll. Um potentielle linguistische Verzerrung zu reduzieren (Präferenzen des Kodierers gegenüber bestimmten Wörtern) wurde die Entscheidung getroffen im ersten Schritt eine In-vivo-Kodierung zu nutzen, bei welcher der zitierte Begriff selbst als Code dient. Nach der vollständigen Kodierung wurden so 153 Codes generiert, welche in 275 Zitaten verankert (grounded) sind. Diese Menge an

Codes erhielt die Bezeichnung „base set“. Im folgenden Schritt wurden Codes zusammengeführt, welche Wordvariationen oder Synonyme darstellten. Die bereinigte Menge („consolidated set“) enthielt 124 Codes. Bei genauer Betrachtung fiel auf, dass viele Codes lediglich einfach durch ein Zitat verankert waren und gegebenenfalls eher als Attribute unter Modellierungsgesichtspunkten verstanden werden würden. So verkörpern die beiden Codes „information in transit“ und „stored information“ lediglich einen Zustand des Konzeptes „information“, welches wiederrum dem Konzept „asset“ zugeordnet werden konnte. Um die Menge der Codes weiter zu reduzieren und auf die Kernkonzepte abzustellen, wurde die Bedingung eingeführt, dass ein Code durch mindestens zwei Zitate verankert werden muss. Der Prozess und das Resultat („core set of codes“) sind in Abbildung 1 dargestellt.

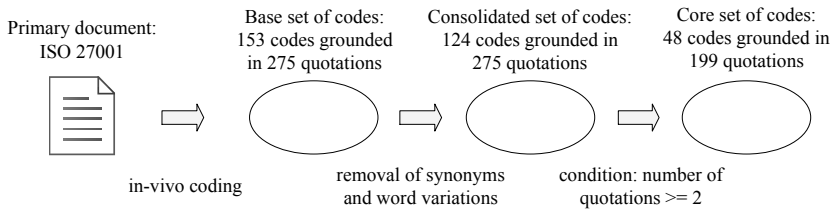

Abbildung 1: Prozess der Kodierung und induktiven Kategorisierung

Die so hergeleiteten Konzepte befinden sich auf der Metamodellebene. Wir definieren Kernkonzepte als Konzepte, welche weder Typen noch Subkonzepte anderer Konzepte sind.

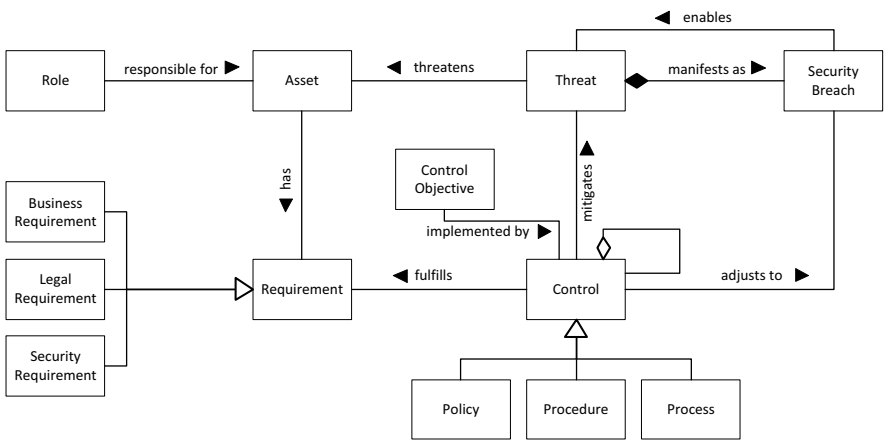

Abbildung 2: ISO 27001 Metamodell

Abbildung 2 zeigt das konstruierte Metamodell des ISO-27001-Standards. Unter den 48 finalen Codes wurden die folgenden Codes als derartige Kernkonzepte identifiziert: „asset“, „threat“, „control“, „requirement“ und „role“. „Assets“, also Vermögensgegenstände, repräsentieren einen Wert, der für die Organisation

schützenswert ist, während „threat“ das Konzept ist, welches diesen Wert gefährdet und „controls“ entsprechend Mittel zur Erreichung des erwähntes Schutzes darstellen.

Das Konzept „requirement“ ist in Form von drei Subkonzepten bzw. Typen vertreten: 1) „security requirement“, 2) „business requirement“ und 3) „legal requirement“. Diese Unterscheidung impliziert eine potentielle Ebenenbetrachtung für die Domäne Informationssicherheit, wie bereits von einigen Forschern suggeriert (siehe [DB01]). Im Vergleich zu den anderen Kernkonzepten finden sich relativ wenige Zitate, welche das Konzept „role“ im Standard verankern. Allerdings ist mit 10 Zitaten das Konzept „responsibility“ stark ausgeprägt, welches die Beziehung zwischen „role“ und „assets“ qualifiziert. Um diesen Indikator für ein Ownership-Paradigma (wie z.B. Process Ownership) nicht zu ignorieren, wurde die Entscheidung getroffen das Konzept „role“ trotz verhältnismäßig schwacher Fundierung mit in das Metamodell aufzunehmen.

Nachdem die fünf Kernkonzepte eingepflegt und „requirement“ und „control“ in ihre Subkonzepte (mit starkem „grounding“ durch Zitate) aufgeteilt wurden, wurden vorher ausgeschlossene Codes mit einfachen Zitaten als Anker re-evaluiert. Hierdurch wurden drei Codes mit einer semantischen Ähnlichkeit identifiziert: „security event“, „security incident“ und „security breach“, welche im Metamodell unter „security breach“ subsummiert wurden. Zwar mag eine Differenzierung über den Grad der Schwere derartiger Ereignisse möglich sein, doch entschied man sich die Codes zusammenzuführen und in das Metamodell aufzunehmen, da eine Analyse der „control“ und „threat“ Konzepte ergab, dass diese Codes eine wichtige Rolle in den Controls A.8.2 (Umgang mit Mitarbeitern, wie z.B. Awareness-Schulungen), A.10.10 (Monitoring) und A.13.2 (Security Incident Management) spielen [In05]. Zuzüglich wurde das Element „control objective“ hinzugefügt, welches eine hohe Bedeutung als strukturelles Element im Standard besitzt. Es ist anzumerken, dass in dem analysierten Teil des ISO 27001 Standards das erwartete Konzept Kennzahlen kaum Beachtung findet, obwohl es eine wichtige Rolle im Rest der ISO 27000-Standardfamilie innehat. Ebenso bestehen kaum Hinweise für eine Zuordnung zwischen den Konzepten „role“ und „controls“ oder „control objectives“. Aus einer Governance-Perspektive wäre die Zuweisung von Verantwortlichkeiten und Entscheidungsrechten bei Implementierung des Standards von hoher Bedeutung.

5 Fazit

Im vorliegenden Beitrag wurden Konzepte der Informationssicherheit hergeleitet. Hierzu fand eine ontologische Metaisierung der Informationssicherheitsmanagementstandards ISO 27001 mithilfe einer induktiven Kategorisierung statt. Hierdurch wurde Einsicht in die Struktur des Standards erreicht. Als methodologisches Werkzeug wurde die Metamodellierung herangezogen und seine grundsätzliche Eignung für Modellvergleiche verargumentiert.

Eine Klärung und Abgrenzung von (ontologischen) Metamodellen und Ontologien fand nicht statt. Aufgrund von Platzgründen wird ein extensiver Vergleich mit mehreren Ontologien in einer Nachfolgepublikation behandelt werden. Die Positionierung von konzeptionellen Modellen, Metamodellen, Referenzmodellen und Ontologien zueinander ist nicht stark erforscht und stellt ein zukünftiges Betätigungsfeld für die Forschung dar. In einer Erweiterung der vorgestellten Arbeit sollen ebenfalls die Instanzen verstärkt betrachtet werden.

Literaturverzeichnis

[BW07] Baker, W. H.; Wallace, L.: Is Information Security Under Control?: Investigating Quality in Information Security Management, IEEE Security and Privacy, 5, 1, 2007, 36-44.

[CS90] Corbin, J. M.; Strauss, A.: Grounded theory research: Procedures, canons, and evaluative criteria, Qualitative Sociology, 13, 1, 1990, 3-21.

[DB01] Dhillon, G.; Backhouse, J.: Current directions in IS security research: towards socio-organizational perspectives, Information Systems Journal, 11, 2, 2001, 127-153.

[GH05] Gitzel, R.; Hildenbrand, T.: A Taxonomy of Metamodel Hierachies. Working paper, Lehrstuhl für ABWL und Wirtschaftsinformatik, 2005.

[Gr95] Grubner, T. R.: Towards principles for the design of ontologies used for knowledge sharing, International Journal of Human-Computer-Studies, 43, 5, 1995, 907-928.

[In05] International Organization for Standardization and International Electrotechnical Commission. Iso/iec 27001:2005, information technology - security techniques - information security management systems- requirements, 2005.

[Le05] Leist-Galanos, S.: Methoden zur Unternehmensmodellierung – Vergleich, Anwendungen und Integrationspotenziale, Logos, Berlin, 2006.

[LG10] Looso, S.; Goeken, M.: Application of Best-Practice Reference Models of IT Governance, Proceedings of European Conference on Information Systems, 2010.

[St96] Strahringer, S.: Metamodellierung als Instrument des Methodenvergleichs. Shaker, Aachen, 1996.

[SW09] Siponen, M.; Willison, R.: Information security management standards: Problems and solutions, Information & Management, 46, 2009, 267-270.

[VHW91] Verhoef, T. F.; Hofstede, A. H. M. T.; Wijers, G. M.: Structuring Modelling Knowledge for CASE Shells. In (Andersen, R. et al. Hrsg.): Proceedings of the third international Conference CAiSE'91 on Advanced Information Systems Engineering, 502-524.