Kontextbasierte Unterstützung des Risikomanagements

Ronny Scholz[1] · Stefan Schemmer[1] · Ralf Schumann[1]

[1]rt-solutions.de GmbH
{scholz, schemmer, schumann}@rt-solutions.de

Zusammenfassung

Risikomanagement, welches sich als ein Kernansatz für das Management der Informationssicherheit etabliert hat, kann nur dann in der erforderlichen Breite und Nachhaltigkeit in Unternehmen realisiert werden, wenn die Durchführung auch dem Nichtexperten mit angemessenem Aufwand möglich ist. Um die Identifikation und Kontrolle von Informationssicherheits-Risiken zu unterstützen, stellen anerkannte Standards Kataloge von Informationswerten, Gefährdungen, Schwachstellen und Maßnahmen bereit. Diese Kataloge sind teilweise sehr umfangreich, so dass eine Auswahl geeigneter Elemente für Nicht-Experten schwierig und aufwändig ist.
Zur Vereinfachung dieser Schritte wird ein Verfahren vorgestellt, dass anhand bereits eingegebener Daten Schlussfolgerungen auf die Relevanz zu verknüpfender Katalogelemente zieht. Als relevant erkannte Datensätze werden priorisiert und dem Benutzer zur Verknüpfung vorgeschlagen.
Eine erste Evaluierung zeigte die Anwendbarkeit des vorschlagsbasierten Ansatzes für die Best-Practice-Kataloge der ISO 27001.

Einleitung

Informations- oder IT-Sicherheit ist nun schon seit geraumer Zeit ein Dauerthema. Die nachhaltige Ausrichtung der IT an den Geschäftszwecken und die Unterstützung der Geschäftsprozesse durch die Bereitstellung sicherer Dienste werden vermehrt als eine Managementaufgabe wahrgenommen, die nur durch geeignete Lenkungsprozesse dauerhaft erfüllt werden kann. Informationsicherheits-Managementsysteme (Information Security Management Systems, ISMS) bieten solche Lenkungsprozesse auf Grundlage von anerkannten Best Practices, namentlich dem ISO Standard 27001. Zu den Kernfunktionen eines ISMS zählen dabei die Verwaltung eines Inventars der Informationswerte und das Risiko-Management, d.h. die Abschätzung des Gefahrenpotenzials von Gefährdungen auf spezifische Schutzziele der Informationswerte sowie die Auswahl und Implementierung geeigneter Schutzmaßnahmen. Für eine systematische Identifizierung von Risiken ist es hilfreich, auf bestehende Best-Practice-Kataloge mit typischen Gefährdungen und Schwachstellen zurückzugreifen. Doch trotz der Nutzung von Best-Practice-Katalogen ist die Durchführung der Risikoanalyse für den Nicht-Experten sehr aufwändig, weil einerseits zu jedem betroffenen Informationswert jeweils sämtliche Gefährdungen und dazu jeweils sämtliche Schwachstellen zu betrachten sind und andererseits eine schnelle und richtige Auswahl Expertenwissen erfordert. Für die Risikobehandlung stehen ebenfalls Best-Practice-Kataloge zur Verfügung, aber auch hier ist aufgrund des

großen Umfangs der Kataloge eine Auswahl geeigneter Sicherheitsmaßnahmen sehr aufwändig. Im Kontext eines momentan bearbeiteten Risikos sind nur sehr wenige der Katalogelemente sinnvoll anzuwenden, so dass der Benutzer mit vielen irrelevanten Auswahlmöglichkeiten konfrontiert wird.

Wünschenswert ist die Unterstützung der Verwaltung des ISMS durch ein Risikomanagement-Tool, welches das Augenmerk des Benutzers auf die relevanten Kombinationen von Informationswerten, Gefährdungen, Schwachstellen und Maßnahmen lenkt und unpassende Elemente herausfiltert.

Das in diesem Beitrag vorgestellte Vorschlagssystem vereinfacht den Prozess der Datenerfassung für das Risikomanagement. Es führt anhand des aktuell betrachteten Risikos und bereits verknüpfter Datensätze eine Kontextanalyse durch und beurteilt über die Abfrage einer Wissensdatenbank die Relevanz noch zu verknüpfender Katalogelemente. Irrelevante Datensätze werden vor dem Benutzer verborgen, so dass dieser mit deutlich weniger Auswahlmöglichkeiten konfrontiert und die Risikoanalyse damit insgesamt beschleunigt wird. Das Vorschlagssystem ist außerdem in der Lage, neben mitgelieferten Katalogelementen auch vom Benutzer manuell eingegebene Informationen zu analysieren und in die Erstellung der Vorschläge einzubeziehen.

Bestehende Verfahren

Obwohl bereits seit einigen Jahren Wissensdatenbanken aufgebaut wurden, um Expertenwissen im Risikomanagement automatisiert zu verarbeiten [KWS+09] [ChKC09], ist AURUM [EkNF09] die einzige uns bekannte Umsetzung in ein Risikomanagement-Tool. Dort soll die Wissensdatenbank dazu beitragen, die Interaktion des Nutzers mit dem Tool zu reduzieren. Dazu setzt AURUM auf eine Ontologie-Datenbank, in der vordefinierte Informationswerte, Gefährdungen, Schwachstellen und Maßnahmen über Gewichtungen miteinander verbunden sind. Damit kann das Tool nach der Eingabe aller spezifischen Unternehmensdaten, z.B. Gebäudeplänen, den darin enthaltenen IT-Geräten und bereits definierten Informationssicherheits-Richtlinien, sehr exakte Verknüpfungen der vordefinierten Katalogelemente erstellen. AURUM unterstützt den Benutzer bei der Bewertung von Eintrittswahrscheinlichkeit und Schadensausmaß von Risiken. So kann es automatisiert den Schweregrad der Risiken ermitteln und vorgeschlagene Maßnahmen priorisieren. Problematisch an diesem Ansatz ist, dass das Risikomanagement des Unternehmens mit den exakten Vorgaben des Tools harmonieren muss. So ist die Nutzung anderer Skalen oder gar eigens erstellter Informationswerte, Gefährdungen, Schwachstellen oder Maßnahmen nicht möglich, weil dafür in der Wissensdatenbank keine Einträge und Verknüpfungen vorgesehen sind. In der Praxis ist allerdings erfahrungsgemäß das Risikomanagement in der Informationssicherheit einem existierenden Umfeld und Kontext anzupassen, z.B. ist hier die Integration in das meist schon bestehende Enterprise Risk Management zu beachten.

Es ist daher ein generischerer Ansatz zu suchen, der sich an das Risikomanagement des Unternehmens anpassen lässt.

Funktionsweise

Während der Risikoidentifikation definiert der Benutzer zunächst einen Namen, eine Beschreibung sowie eine Kategorie für das Risiko. Diese Eingaben bilden den Kontext bzw. das semantische Wissen des Risikos, das für die Generierung von Vorschlägen für die Verknüpfung von Informationswerten herangezogen wird. Nachdem der Benutzer die vorgeschlagenen Informationswerte mit dem Risiko verknüpft hat, werden diese ebenfalls in den Kontext aufgenommen und zur Generierung von Vorschlägen für weitere Verknüpfungen verwendet. Auf diese Weise vergrößert sich das semantische Wissen zum Risiko mit jeder weiteren Eingabe des Benutzers. So fließen in die Vorschläge für Sicherheitsmaßnahmen nicht nur Name, Beschreibung und Kategorie des Risikos ein, sondern auch bereits verknüpfte Informationswerte, Schwachstellen und Gefährdungen.

Das hier dargestellte Verfahren ist nicht spezifisch für die Domäne der Informationssicherheit und lässt sich auch auf andere Domänen anwenden. Aus diesem Grund werden im Folgenden einzelne Katalogelemente von Informationswerten, Gefährdungen, Schwachstellen und Maßnahmen sowie manuell vom Benutzer eingegebene Informationen allgemein als Datensatz bezeichnet. Das Verfahren besteht aus zwei Phasen, einer Vorverarbeitung und der eigentlichen Generierung von Vorschlägen. Während der Vorverarbeitung werden zu jedem Datensatz zusätzliche Informationen bestimmt, die zur Generierung der Vorschläge herangezogen werden. Beide Phasen werden im Folgenden detailliert erläutert.

Vorverarbeitung

Das Wissen über ein Risiko besteht aus einer Repräsentation aller bereits angegebenen Informationen, d.h. Angaben zum Risiko selbst und verknüpfte Datensätze. Dieses datensatzspezifische Wissen besteht aus den Schlagworter, d.h. repräsentativen Wörtern, der einzelnen Datenfelder. So fließen in die Schlagworte zu einem Informationswert Informationen aus dessen Name, Beschreibung und Kommentaren ein. Die ermittelten Schlagworte werden als neues Feld des Datensatzes gespeichert. Da ein Datensatz während des Risikomanagements nur selten verändert wird, kann die Erzeugung der Schlagworte im Vorfeld der Vorschlagsgenerierung durchgeführt werden. Dazu werden die Schlagworte eines Datensatzes bei jeder Änderung nach dem im Folgenden beschriebenen Schema generiert.

Die einzelnen Schlagworte eines Datensatzes werden mittels Konzepten des Information Retrieval, d.h. anhand einer Wortanalyse gewonnen (Abb. 1). Dazu werden die signifikanten Felder des Datensatzes (z.B. Name, Beschreibung und bereits verknüpfte Daten) zusammengeführt und in einzelne Wörter aufgetrennt. Die Liste der ermittelten Wörter enthält noch viele Einträge ohne Aussagekraft, zum Beispiel Artikel und Präpositionen. Diese Wörter werden anhand einer vordefinierten Stoppwort-Liste herausgefiltert. Die verbleibenden Wörter bilden zwar bereits den Kontext des Datensatzes, sind aber für eine maschinelle Auswertung noch nicht geeignet. Denn für eine Suchanfrage in der Wissensdatenbank müssen die Schlagworte

exakt mit den dort gespeicherten Daten übereinstimmen. Die Schlagworte können allerdings noch verschiedene Beugungsformen aufweisen, so dass sie zwar inhaltlich identisch, aber dennoch unterschiedlich sind. Im letzten Schritt der Vorverarbeitung führt das Vorschlagssystem daher eine Reduktion der verbleibenden Wörter auf ihre Grundform durch. Dies geschieht durch die Abfrage eines speziellen Lexikons. So werden beispielsweise die Wörter „Vorfall“, „Vorfalls“ und „Vorfälle“ auf „Vorfall“ reduziert. Die ermittelten Grundformen bilden die Schlagworte des Datensatzes. Sie sind vom Benutzer einsehbar und können ggf. angepasst werden. Da die Schlagwortgenerierung auf rein textueller Ebene arbeitet, werden auch benutzerdefinierte Datensätze vom Vorschlagssystem vollständig unterstützt. Das Unternehmen ist damit in der Lage, neben der Nutzung von Best-Practice-Katalogen beispielsweise auch eigene Gefährdungen zu definieren und das Risikomanagement besser auf den spezifischen Anwendungsfall auszurichten.

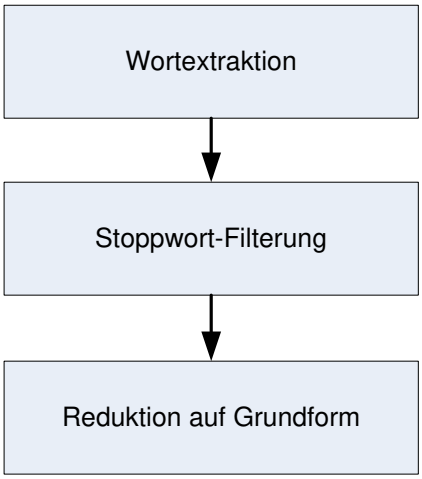

Abb. 1: Ablauf der Schlagwortextraktion

Erstellen von Vorschlägen

Die Generierung von Vorschlägen erfolgt während der Bearbeitung einzelner Risiken durch den Benutzer. Während der Dateneingabe zu einem Risiko gibt der Benutzer betroffene Informationswerte und deren Schwachstellen, sowie Gefährdungen und Sicherheitsmaßnahmen an. Für jede dieser Angaben wird er vom Vorschlagssystem unterstützt. Dazu werden anhand bereits angegebener Verknüpfungen die Listen verbleibender Datensätze gefiltert, um deren Auswahl zu vereinfachen. Die einzelnen Schritte der Vorschlagsgenerierung werden in Abbildung 2 dargestellt und nachfolgend erläutert.

Zunächst wird der aktuelle Kontext bestimmt. Dieser besteht aus allen Schlagworten des momentan betrachteten Risikos sowie bereits verknüpfter Datensätze. Anschließend werden über eine Wissensdatenbank zusätzliche Schlagworte herausgesucht, die zum aktuellen Risiko relevant sind. Da die gefundenen Schlagworte auch zur Beschreibung anderer Katalogelemente gehören, kann somit deren Relevanz zum aktuellen Risiko bewertet werden. Wurden Schlag-

worte eines bisher unverknüpften Katalogelements gefunden, so ist es relevant und wird dem Benutzer zur Verknüpfung vorgeschlagen, andernfalls wird es ausgeblendet. Es besteht jedoch die Möglichkeit, die als irrelevant eigestuften Datensätze in einer separaten Ansicht zu betrachten.

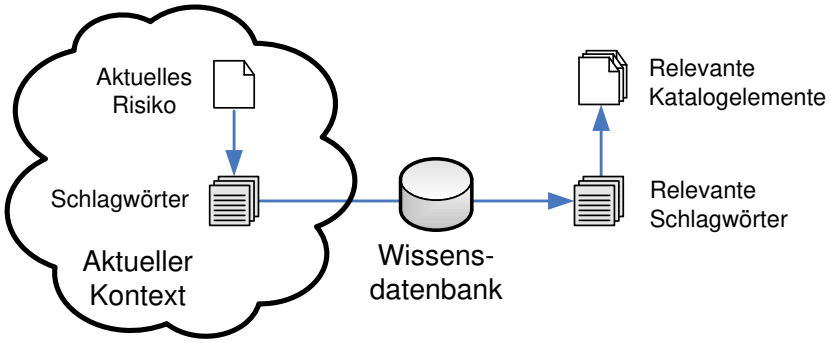

Abb. 2: Bestimmung relevanter Datensätze für den aktuellen Kontext

Die Wissensdatenbank speichert Schlagworte aus dem Umfeld der Informationssicherheit und ihre Beziehungen untereinander. Abbildung 3 zeigt die netzwerkähnliche Struktur der Wissensdatenbank. Idealerweise ist jedes Schlagwort mit jedem anderen Schlagwort direkt oder indirekt verbunden. Schlagworte sind umso relevanter zueinander, je kleiner der minimale Abstand zwischen ihnen ist.

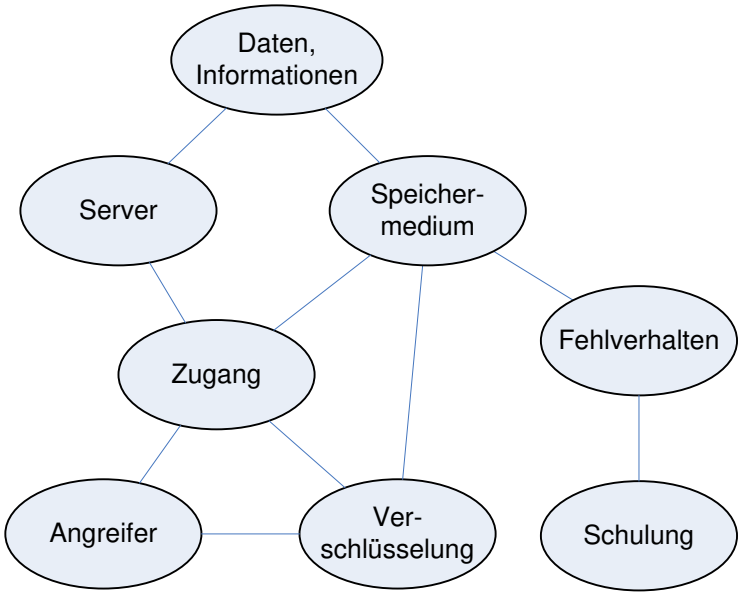

Abb. 3: Auszug der Wissensdatenbank

Eine Suche in der Wissensdatenbank liefert alle Schlagworte zurück, die direkt mit den Eingabewörtern in Beziehung stehen oder über wenige weitere Schlagworte miteinander verknüpft sind. Da die Schlagworte der Ergebnisliste ihrerseits andere Datensätze beschreiben, lassen sich so die relevanten Datensätze zum aktuellen Kontext, d.h. zum aktuell betrachteten Risiko, ermitteln.

Der Grad der Relevanz wird über die Anzahl übereinstimmender Schlagworte und ihren Abstand zum Eingabekontext in der Datenbank hergeleitet. Er wird zur Sortierung der Vorschlagsliste herangezogen, so dass die relevantesten Datensätze oben stehen.

Die Genauigkeit der Vorschläge hängt von der Ausführlichkeit der Beschreibung der Datensätze sowie der Qualität der Wissensdatenbank ab. Deswegen verlangt das Vorschlagssystem vom Benutzer eine explizite Bestätigung oder Modifikation der Vorschläge, bevor diese als Verknüpfung in das ISMS übernommen werden.

Zur Erstellung der Wissensdatenbank verwendeten wir die Daten der BSI-Bausteine, da diese bereits Empfehlungen für typische Verknüpfungen von Informationswerten mit Gefährdungen, Schwachstellen und Maßnahmen geben und diese Daten bereits sehr ausführlich beschrieben sind. Zunächst wurden für alle BSI-Datensätze die Schlagworte generiert. Für die anschließende Stoppwort-Extraktion und Reduktion auf die Wort-Grundform existieren keine frei verfügbaren Listen in deutscher Sprache. Daher mussten diese Listen manuell erstellt werden. Die so extrahierten Schlagworte wurden automatisiert in die Wissensdatenbank eingetragen und anhand der Empfehlungen der BSI-Bausteine zunächst direkt miteinander verknüpft. Um die Komplexität der Wissensdatenbank zu reduzieren, wurden anschließend einige der Direktverbindungen manuell wieder entfernt. Das ist möglich, weil Schlagwörter auch dann noch als relevant eingestuft werden, wenn sie über wenige Zwischenverbindungen erreichbar sind.

Konfiguration

Die Konfiguration des Vorschlagssystems erfolgt größtenteils vom Hersteller des Risiko-Management-Tools. Er definiert, auf welche Weise Schlagworte gebildet werden. Dazu gehört einerseits die Definition verbotener Wortarten und Wörter, andererseits die Erstellung des Lexikons zur Wortstammbildung. Er modelliert außerdem die Wissensdatenbank und legt folgende Parameter fest:

- Bis zu welcher Suchtiefe D_{max} werden Schlagworte als relevant eingestuft? Die Suchtiefe entscheidet über die Anzahl der Vorschläge und sollte daher nicht zu groß gewählt werden. Eine Tiefe von 3 ist für die BSI-Kataloge ausreichend.
- Mit welcher Formel wird die Relevanz R eines Datensatzes berechnet? Mögliche Einflussgrößen sind Abstand D und Anzahl N der übereinstimmenden Schlagworte. Als einfache Formel eignet sich beispielsweise $R = \Sigma(D_{max} - D + 1)$ über alle übereinstimmenden Schlagworte.

Diese Definitionen sind mit viel Fingerspitzengefühl durchzuführen, weil sie die Qualität der Vorschläge signifikant beeinflussen. Für den Benutzer des Risikomanagement-Tools ergibt sich jedoch der Vorteil, dass er das System ohne Konfiguration sofort einsetzen kann.

Gibt der Benutzer während der Risikoidentifikation neue Datensätze ein, entscheidet die Qualität der Beschreibungstexte darüber, ob sinnvolle Vorschläge erstellt werden können. Da der Benutzer jedoch keine Kenntnis von der internen Struktur der Wissensdatenbank hat und somit die Güte der Beschreibungen nicht abschätzen kann, bietet das Vorschlagssystem zwei Möglichkeiten, zur Laufzeit Einfluss auf die Erstellung der Vorschläge zu nehmen.

Die erste Möglichkeit besteht darin, die Struktur der Wissensdatenbank selbst anzupassen. Dies kann immer dann geschehen, wenn der Benutzer Datensätze verknüpft, die vom Vorschlagssystem fälschlicherweise als irrelevant eingestuft wurden. Das System präsentiert in diesem Fall eine Liste der beteiligten Schlagworte, die als relevant markiert werden können, von denen der Benutzer eine oder mehrere aus seiner Sicht relevante Kombinationen auswählt. Diese Kombinationen werden als Verknüpfung in die Wissensdatenbank eingetragen und fließen in weitere Vorschläge ein. Auf diese Weise kann das Vorschlagssystem auf das spezifische Anwendungsszenario trainiert werden.

Die zweite Möglichkeit besteht in der Modifikation der maximalen Suchtiefe D_{max}. Dieser Parameter hat eine unmittelbare Auswirkung auf alle Vorschläge, weil sie die Anzahl der für relevant befundenen Schlagworte steuert. Dazu ist während der Risikoidentifikation zunächst zu überprüfen, ob die vorgeschlagenen Datensätze noch sinnvoll sind. Bei Abweichungen kann die maximale Suchtiefe gemäß Tabelle 1 angepasst werden.

Tabelle 1: Anpassung der maximalen Suchtiefe D_{max}

Aktueller Status	Anforderung	Benötigte Modifikation
Das Risikomanagement-Tool schlägt nicht alle gewünschten Katalogemenete für eine Verknüpfung vor.	Das Risikomanagement-Tool sollte mehr Katalogelemente für eine Verknüpfung vorschlagen.	Erhöhung der maximalen Suchtiefe für Schlagworte, bis alle gewünschten Katalogelemente vorgeschlagen werden.
Das Risikomanagement-Tool schlägt zu viele irrelevante Verknüpfungen vor. Alle gewünschten Verknüpfungen werden allerdings vorgeschlagen.	Das Risikomanagement-Tool sollte weniger Verknüpfungen vorschlagen.	Verringerung der maximalen Suchtiefe und anschließende Überprüfung, dass nach wie vor alle gewünschten Verknüpfungen vorgeschlagen werden.

Zusammenfassung und Ausblick

Das vorgestellte Vorschlagssystem dient der Vereinfachung der Risikoidentifizierung und Maßnahmenauswahl, indem es den Benutzer mit Vorschlägen für Auswahlmöglichkeiten unterstützt. Dazu wird über eine Textanalyse semantisches Wissen über alle Auswahlmöglichkeiten gesammelt. Anhand bereits getroffener Verknüpfungen mit Datensätzen ist der aktuelle Kontext bekannt. Davon ausgehend erfolgt die Schlussfolgerung auf weitere relevante Datensätze über eine Wissensdatenbank, die Verknüpfungen informationssicherheits-relevanter

Wörter speichert. So können auch weitere, vom Benutzer eingegebene Informationen automatisch vom Vorschlagssystem erfasst werden, was die Handhabbarkeit beim Einsatz in konkreten Anwendungsfällen deutlich verbessert. Damit unterscheidet sich das hier vorgestellte Vorschlagssystem von anderen Ansätzen, deren Wissensdatenbank die Datensätze aus der Informationssicherheit direkt miteinander verbindet.

Obwohl die Wissensdatenbank mit den Daten des BSI-Grundschutzkataloges kalibriert wurde, haben erste Evaluierungen gezeigt, dass das Vorschlagssystem auch auf anderen Best-Practice-Katalogen sowie manuell eingegebenen Datensätzen sinnvolle Vorschläge generiert. Somit ließ sich unter anderem die mehr als einhundert Elemente umfassende Maßnahmenliste von ISO 27002 für die jeweils betrachteten Risiken auf eine Handvoll relevanter Maßnahmen reduzieren. Für umfangreichere Testläufe wird das Vorschlagssystem ein Risikomanagement-Tool, den „Risk-Manager“, integriert.

Bei der Priorisierung von Maßnahmen ist eine Bewertung anhand der ermittelten Relevanz allein nicht ausreichend. Vielmehr sollten Maßnahmen auch anhand weiterer Kriterien priorisiert werden, wie etwa der generellen Anwendbarkeit im Unternehmen oder des Verhältnisses von Nutzen und Aufwand [Mahr09]. Dadurch kann die Betrachtung des Benutzers schneller auf Maßnahmen gelenkt werden, die tatsächlich umsetzbar sind.

Durch die Unterstützung von Nicht-Experten während der Risikoidentifikation eignet sich das Vorschlagssystem auch für den Einsatz in Branchen, in denen Risikomanagement bisher eine untergeordnete Rolle gespielt hat. Beispielsweise kann es in der Automatisierung zur Beantwortung der Fragestellung dienen, welche Gefährdungen mit der Nutzung einer neuartigen Technologie einhergehen. Für diese Benutzergruppe wurde ein Referenzmodell entwickelt, das auf dem Vorschlagssystem beruht und vom Hersteller der Automatisierungstechnologie bereits mit den Daten eines generischen Anwendungsszenarios vorkonfiguriert wird [ISSS10]. Das Referenzmodell wird im Rahmen des Forschungsprojektes flexWARE prototypisch implementiert und in verschiedenen Einsatzszenarien weiter evaluiert.

Literatur

[KWS+09] S. Kollarits, N. Wergles, H. Siegel, C. Liehr, und weitere: MONITOR-an ontological basis for risk management (2009)

[ChKC09] T.J. Chiang, J.S. Kouh, R.I. Chang: Ontology-based Risk Control for the Incident Management, In: IJCSNS Vol. 9. (2009)

[EkNF09] A. Ekelhart, T. Neubauer, S. Fenz: Automated risk and utility management, In: Proceedings of the 2009 Sixth International Conference in Information Technology: New Generations (2009)

[Mahr09] D. Mahrenholz: Return On Security Investment: Ein Konzept zur Bewertung von Sicherheitsmaßnahmen, In: VDMA Nachrichten (2009)

[ISSS10] S. Ivanov, R. Scholz, S. Schemmer, R. Schumann: Security Standardtechnologien in der Automatisierung: Ein Referenzmodell hilft bei der risikobasierten Maßnahmenauswahl. In: atp – Automatisierungstechnische Praxis (2010)